Ministerie van Onderwijs, Cultuur
en Wetenschap

Samenvatting beleidslijn archivering chatberichten

Project chatarchivering

Versiebeheer

September 2025	Versie t.b.v. behoeftesessie departementen
November 2025	Versie t.b.v. bespreking in IEO-IHH
15 januari 2026	Versie t.b.v. advisering in IEO-IHH
6 februari 2026	Versie t.b.v. behandeling in Programmaraad
x.x datum-maand-jaar	Versie t.b.v. (gremium)
x.x datum-maand-jaar	Versie t.b.v. (gremium)

Inhoud

1. Inleiding

Deze samenvatting heeft als doel om op hoofdlijnen inzicht te geven in de beleidslijn *Archivering chatberichten Rijksoverheid* en om duidelijk te maken welke eisen, afspraken en verantwoordelijkheden hieruit voortvloeien voor organisaties binnen de Rijksdienst. De samenvatting is bedoeld als praktisch hulpmiddel om snel te kunnen bepalen wat organisaties zelf moeten doen om aan de beleidslijn te voldoen en zich voor te bereiden op de implementatie.
De samenvatting is primair bedoelt voor:

- Projectleiders;
- Cio's, CDO's en informatiemanagers;
- Beleidsmedewerkers en adviseurs informatiehuishouding;
- Uitvoerende functionarissen die betrokken zijn bij de inrichting, implementatie en naleving van het beleid.

Aanleiding

De beleidslijn archivering chatberichten Rijksoverheid (versie 1.0, april 2025) is een bindend beleid voor alle organisaties van de Rijksdienst. De aanleiding om dit beleid op te stellen is de uitspraak van de Raad van State (2019), waarin is vastgesteld dat sms- en WhatsAppberichten onder de definitie van 'document' vallen zoals gehanteerd onder de Wet Openbaar Bestuur (inmiddels Wet Open Overheid). Het maakt daarbij niet uit of de berichten op een zakelijke of privételefoon van een ambtenaar staan. Zowel de Raad van State, de parlementair advocaat als de Inspectie Overheidsinformatie en Erfgoed kwamen vervolgens tot de conclusie dat wanneer chatberichten 'naar hun aard' zijn bestemd om te berusten bij het overheidsorgaan, zij ook archiefbescheiden zijn. Anders gezegd, alle chatberichten die betrekking hebben op de uitvoering van taken van het overheidsorgaan vallen onder het toepassingsbereik van de Archiefwet. In de Archiefwet is dit aangeduid met de term 'archiefbescheiden'. Dat betekent dat alle chatberichten van een ambtenaar of bestuurder van een overheidsorgaan, waarbij gegevens worden vastgelegd die het functionele handelen van de ambtenaar of bestuurder betreffen, onder de reikwijdte van de Archiefwet vallen. De vorm van de informatie doet er voor de wet niet toe.

Doel

De beleidslijn heeft als doel de informatiehuishouding van de Rijksoverheid te versterken door te zorgen voor een toekomstbestendige en uniforme aanpak van het archiveren van zakelijke chatberichten van de rijksoverheid. Dit houdt in dat zakelijke chatberichten duurzaam toegankelijk maken middels archivering conform de eisen van de Archiefwet, de Wet open overheid (Woo), de Algemene Verordening Gegevensbescherming (AVG) en andere relevante regelgeving.

Scope

De beleidslijn richt zich specifiek op de archivering van chatberichten die worden verstuurd via commerciële of informele communicatiekanalen waarbij de zakelijke chatberichten zich niet bevinden in een door de organisatie beheerd informatiesysteem. Denk hierbij aan voorzieningen zoals WhatsApp en Signal en SMS. Deze chatapps worden veelvuldig gebruikt op werk- of privételefoons.
De beleidslijn is bedoeld voor ministeries, maar kan ook worden gebruikt door andere Rijksoverheidsorganisaties en is toepasbaar op:

- Alle typen berichtenapps (WhatsApp, Signal, SMS, etc.) via een mobiele app voor instant messaging ontwikkeld voor de smartphone (veelal gekoppeld aan een telefoonnummer) of websites met een geïntegreerde chatvoorziening;
- Alle soorten chatgesprekken (zowel appgroepen als één-op-één gesprekken).in via mobiele apps.

Het beleid is door de ICBR vastgesteld voor de Rijksdienst. Ministers borgen dit beleid binnen ZBO's via de jaargesprekken met de ZBO's die onder verantwoordelijkheid van de betreffende minister vallen.
De volgende vormen van communicatie vallen buiten de scope van deze beleidslijn:

- Chatberichten via samenwerkingsplatformen: deze wordt via de beleidslijn voor de werkomgeving van de Rijksoverheid meegenomen.
- Chatberichten via socialemediakanalen: chat is daar slechts een ondersteunende functie en wordt via de beleidslijn sociale media meegenomen.

Inwerkingtreding

Tot de formele inwerkingtreding van de nieuwe beleidslijn blijft de *Tijdelijke instructie chatberichten voor bewindspersonen* van kracht. Organisaties kunnen tot het moment dat de beleidslijn in werking is getreden zelf afwegen of zij de werkwijze uit de oude handreiking nog willen blijven gebruiken of voor (een deel van de) sleutelfuncties (bijvoorbeeld in schaal 18–19) chatgesprekken integraal willen laten veiligstellen volgens de tijdelijke instructie chatberichten voor bewindspersonen. Het is in de huidige beheersituatie niet uitvoerbaar om dit voor alle (potentiële) sleutelfuncties te doen. CIO Rijk onderschrijft dat dit een groeimodel is waar organisaties op basis van realistische en uitvoerbare keuzen een eigen afweging maken.

De beleidslijn treedt pas in werking als aan de volgende voorwaarden is voldaan:

1. Er is een samenvatting van de beleidslijn beschikbaar die duidelijk maakt welke eisen en afspraken gelden. Hieruit moet blijken wat organisaties zelf moeten doen.
2. De totaalplanning en uitvoeringsconsequenties en financiële impact zijn in kaart gebracht.
3. De beleidslijn is goedgekeurd door zowel de ICBR als de Gezamenlijke Ondernemingsraad Rijk (GOR);
4. De rijksbrede voorziening is getest, functioneel en beschikbaar vóór de ingangsdatum van de nieuwe Archiefwet.

Het CIO-beraad neemt het formele GO/NO GO-besluit over de inwerkingtreding van de beleidslijn. Vanaf dat moment zijn Rijksorganisaties verplicht tot toepassing van de sleutelfunctiebenadering. Afwijken is alleen mogelijk op basis van het comply or explain principe. De beleidslijn en de bijbehorende selectielijsten worden in de praktijk toegepast zodra de generieke voorziening beschikbaar is. Vanaf dat moment wordt ook gestart met monitoring op naleving, met ruimte voor zorgvuldige procesinrichting en ondersteuning. Voor de omgang met de legacy (eerder niet-automatisch veiliggestelde chatberichten) wordt een separate beleidslijn opgesteld.

Groeimodel

De beleidslijn archivering chatberichten moet gezien worden als een eerste stap in een groeimodel. De ambitie is om deze beleidslijn chat in de toekomst op te nemen in één overkoepelende beleidslijn voor de digitale werkomgeving.

2. Beleid

Kernpunten van het beleid

De beleidslijn bouwt voort op de kabinetsreactie uit april 2023 en introduceert een 'by design'-oplossing van chatarchivering, gebaseerd op de Capstone-selectiemethode (ook wel sleutelfunctie-methode genoemd). Deze selectiemethode is gebaseerd op het uitgangspunt dat sleutelfuncties zogenoemde informatie-knooppunten zijn waar informatie van de gehele organisatie op een centraal punt bij elkaar komt. Door die informatie te bewaren valt het handelen van de organisatie op hoofdlijnen te reconstrueren.

Belangrijke uitgangspunten zijn:

- Archivering is gekoppeld aan functie, niet aan inhoud, dossier of zaak.
- De methode maakt geautomatiseerde archivering mogelijk, mits zorgvuldig ingericht en toegespitst op de context van de organisatie.
- Privé en partijpolitieke communicatie moeten gescheiden worden van zakelijke communicatie om geautomatiseerde opslag uitvoerbaar te kunnen maken. Alleen zakelijke communicatie moet gearchiveerd worden.
- Zakelijke chatberichten van medewerkers in een sleutelfunctie worden automatisch veiliggesteld.
- Voor andere functies geldt een lichtere benadering, afhankelijk van informatiewaarde.
- Er zijn voldoende privacymaatregelen genomen, zoals het verwijderen of uitfilteren van privéberichten, conform AVG-eisen en in lijn met dataminimalisatie.
- Organisaties moeten de regels volgen op basis van het '*comply or explain*-principe': afwijken van de gestelde regels mag alleen gemotiveerd.

We onderscheiden twee uitzonderingen op het geautomatiseerd veiligstellen van chatgesprekken overeenkomstig de Capstone-methodiek.

- Dit betreft chatgesprekken van specifieke soorten functies die standaard werken met gevoelige of bijzondere privé (persoons)gegevens. Dit wordt nader toegelicht in paragraaf 2.3 van de beleidslijn.
- Dit betreft chatberichten van Politiek Assistenten (PA's). De functie van PA richt zich voor een belangrijk deel op partijpolitieke aangelegenheden, deze informatie hoort niet tot het organisatiearchief en moet worden uitgesloten van bewaring. Hierdoor komen zij in aanmerking voor uitzondering op het beoogde geautomatiseerd veiligstellen van chatberichten overeenkomstig de Capstone-methodiek.

Daarmee is zeker niet gezegd dat chatberichten van de uitzonderingsfuncties buiten het bereik vallen van de Archiefwet. Voor deze functies is het aan te raden vast te houden aan handmatige selectie en archivering van zakelijke chatberichten. Indien gewenst kan geautomatiseerd veiligstellen alsnog plaatsvinden.

Algemene beleidsuitgangspunten voor overheidsinformatie

Algemene beleidsuitgangspunten hebben een communicatiemiddel en -voorziening overstijgende werking en bevorderen archivering, openbaarheid, privacy, veiligheid en uitvoerbaarheid. Algemene beleidsuitgangspunten relevant voor chatgesprekkenarchivering zijn:

- Eindgebruikers van overheidsmiddelen en -systemen scheiden hun privé en partijpolitieke informatie waar mogelijk van zakelijke informatie, om het informatiebeheer uitvoerbaar te kunnen houden.
- Overheidsorganisaties zijn bij of krachtens de wet zelf belast met de zorg voor hun documenten, maar beleid en afspraken worden zoveel mogelijk rijksdienst- dan wel overheidsbreed vastgelegd of tenminste in afstemming tussen de verschillende overheidslagen.
- Besluiten over waardering en selectie zijn (conform de Archiefwet) in selectielijsten vastgelegd. Wanneer de inzet van een selectiemethodiek op basis van werkprocessen niet mogelijk of wenselijk is, kan er voor worden gekozen om gebruik te maken van een selectiemethodiek op basis van

informatieknooppunten, de zogenoemde Capstone-methodiek . De Algemene Rijksarchivaris vervult hier een richtinggevende rol in vanwege de verantwoordelijkheid voor de eenheid van selectiebeleid.
- Nieuwe communicatiemiddelen en informatiesystemen moeten, mits er sprake is van overheidsinformatie in de zin van de Archiefwet en de Woo, duurzame toegankelijkheid en archivering, privacy en openbaarmaking by design afdwingen
- Informatie wordt structureel, als geheel en zoveel mogelijk geautomatiseerd verwerkt en voldoende veilig (conform BIO, VIR en VIR-BI) en conform AVG beheerd.
- Er zijn heldere regels en procedures om documenten die onder de noemer 'privé' of 'partijpolitiek' vallen, uit te zonderen van bewaring. Dit wordt opgenomen in een afwegingskader dat ondersteunend aan de beleidslijn door CIO Rijk wordt ontwikkeld.
- Organisaties bouwen voldoende controles en verplichte audits in het informatiebeheer in om aan te kunnen tonen dat het archief- en informatiebeheerbeleid aantoonbaar wordt nageleefd.
- Rijksoverheidsorganisaties zorgen ervoor dat als er sprake is van een behoefte om gevoelige informatie (zoals commercieel vertrouwelijk of diplomatiek verkeer) of zelfs informatie op staatsgeheim niveau te delen of te bewaren, zij hier voorzieningen voor beschikbaar stellen. Zij zorgen daarbij ook dat de informatie op een voldoende veilige wijze wordt beschermd. Daarnaast zal ook de beheerde informatieverzameling als geheel beoordeeld moeten worden op gevoeligheid en passend beschermd moeten worden. Totaalverzamelingen van chatberichten en contactgegevens van sleutelfuncties kunnen van waarde zijn voor statelijke actoren of criminele organisaties. Indien noodzakelijk worden hier via CIO Rijk rijks(dienst)brede bindende afspraken over gemaakt.

Specifieke beleidsregels voor chat

Specifieke beleidsregels voor chatberichtenarchivering zijn:
- Besluiten over waardering en selectie zijn (conform de Archiefwet) in selectielijsten vastgelegd. Het kabinet heeft ervoor gekozen om voor de archivering van chatberichten gebruik te maken van een selectiemethodiek op basis van informatieknooppunten, de zogenoemde Capstone-methodiek.
- Voor chatgesprekken is een model selectielijst chat op basis van sleutelfuncties op- en vastgesteld. In de model selectielijst staat wat de bewaartermijn is van de documenten van zowel sleutelfuncties als niet-sleutelfuncties. Rijksoverheidsorganisatie stellen een eigen selectielijst op basis van de model selectielijst chat op.
- Chatgesprekken met een bij wet gestelde bewaartermijn worden na het verstrijken van deze termijn vernietigd.
- De organisatie slaat de zakelijke chatgesprekken van sleutelfuncties of functies waarvan de chatgesprekken een lange bewaartermijn (> 1 jaar) hebben toegekend, structureel op in een centraal of door de organisatie beheerd systeem en/of omgeving. Het gaat dan om de chatberichten van bewindspersonen, bestuurders en de ambtelijke top. Dit moet niet handmatig en per stuk gebeuren, maar structureel, als geheel en zoveel mogelijk geautomatiseerd ondersteund door informatieprofessionals.
- Een uitzondering op het geautomatiseerd veiligstellen van chatgesprekken overeenkomstig de Capstone-methodiek vormen chatgesprekken van specifieke soorten functies die standaard werken met gevoelige of bijzondere privé (persoons)gegevens (zie ook paragraaf 2.3 van de beleidslijn).
- Bewindspersonen, Rijks- en defensieambtenaren scheiden privé-, partijpolitieke en zakelijke communicatiestromen door privé en partijpolitieke chatberichten zo min mogelijk via zakelijke middelen en voorzieningen uit te wisselen. Dit zorgt ervoor dat aan de voorkant privé- en partijpolitieke chatberichten worden gescheiden van zakelijke chatberichten die voor archivering in aanmerking komen, waardoor intensieve en kostbare handmatige bewerking van het organisatiearchief achteraf wordt beperkt.
- Bewindspersonen, Rijks- en Defensieambtenaren delen geen bijzondere persoonsgegevens (zoals medische informatie via chatapplicaties). Ook is het niet toegestaan om andere vertrouwelijke of gerubriceerde informatie te delen via berichtenapps. Uitzonderingen hierop zijn enkel mogelijk als dit door de organisatie via vastgesteld beleid expliciet is toegestaan in verband met een goede uitvoering van de wettelijke taak en hier specifieke zakelijke middelen en voorzieningen voor zijn aangewezen.
- (Bijzondere) persoonsgegevens en documenten met persoonsgegevens mogen alleen worden verwerkt als hier een wettelijke grondslag voor is. En als die er niet is, worden ze verwijderd of gelakt (bij informatieverzoeken).
- Vertrouwelijke en gerubriceerde informatie mag alleen worden verwerkt voor zoverre de voorschriften, regelingen en baselines dat toestaan (o.a. VIR, VIR-BI, BIO) en moet via daarvoor geschikte middelen verlopen. Veelal heeft dit als consequentie dat er geen vertrouwelijke en gerubriceerde informatie via

commerciële chatapplicaties gedeeld mag worden. De CISO (office) van de organisatie kan hier uitsluitsel over geven.

- Verwijdering van zuiver privé- en partijpolitieke chatberichten binnen de opgeslagen zakelijke chatgesprekken in de beheerde systemen van de organisatie wordt uitgevoerd door de berichteneigenaar c.q. sleutelfunctie. Zij worden hierbij in staat gesteld om:
  - zuiver privé of partijpolitieke chatgesprekken (die niet uit hoofde van functie zijn verstuurd of ontvangen) op contactpersoon niveau te verwijderen uit de eigen veiliggestelde chatgesprekken.
  - zuiver privé of partijpolitieke chatberichten te verwijderen uit de eigen veiliggestelde chatgesprekken

Bovenstaande geldt voor zoverre dit technische mogelijk is en de beheerslast proportioneel is ten opzichte van het gelopen risico.

- Zakelijke chatgesprekken worden veilig en voorzien van waarborgen opgeslagen, zodat alleen bevoegden hier (tijdelijk) toegang toe hebben.
- Voor de toegang tot de veiliggestelde e-mails en chatgesprekken dient een aparte regeling te worden vastgesteld, waarin (onder meer) de voorwaarden en toe te passen hulpmiddelen staan beschreven. Toegang dient in ieder geval strikt beperkt te zijn tot de reikwijdte van het betreffende informatieverzoek.
- Organisaties kunnen daarnaast ter ondervanging van onderlinge verschillen nadere (gedrags-)regels stellen, zolang deze niet conflicteren met de regels die op Rijksoverheidsniveau zijn vastgesteld.

3. Gedragsregels en chatgebruik

Een heldere gedragslijn is essentieel om te zorgen dat alleen zakelijke communicatie duurzaam wordt opgeslagen en openbaar kan worden gemaakt.

Gebruiksregels

Van rijksmedewerkers en bewindspersonen wordt verwacht dat zij actief bijdragen aan het scheiden van communicatievormen. Dit leidt ertoe dat middelenscheiding verplicht is. De ICBR heeft op 4 juli 2023 besloten er voor zorg te dragen dat bewindspersonen, waar dit nog niet gebeurd is, per direct voorzieningen gaan treffen om zakelijke communicatie te scheiden van privé en partijpolitieke communicatie. Dit middels de toepassing van een privé telefoon en een zakelijke telefoon (voor zakelijk berichtenverkeer).

De belangrijkste regels voor medewerkers zijn:

- Gebruik chat niet voor het delen van medische gegevens, personeelsgegevens, persoonsgegevens en voor formele zaken, zoals bestuurlijke besluitvorming.
- Scheid privé, partijpolitieke en zakelijke conversaties. Maak gebruik van een privé-telefoon voor privé en partijpolitieke communicatie.

Deze gedragsregels zijn verwerkt in bestaande kaders, waaronder de gedragsregeling voor de digitale werkomgeving voor Rijksambtenaren en het Handboek Bewindspersonen.

4. Privacy en juridische waarborgen

Juridische toetsing

De mitigerende maatregelen uit de DPIA op de beleidslijn en maatregelen voortvloeiend uit het advies van de Landsadvocaat zijn hier opgenomen om te voorkomen dat meer persoonsgegevens worden verwerkt dan noodzakelijk, en om de impact op de persoonlijke levenssfeer te beperken.

Privacymaatregelen

- Organisaties zijn verplicht om de bewindspersonen en medewerkers doorlopend te informeren en instrueren over de werkwijze, en deze ook op te nemen in het onboardingsproces.
- Chatgesprekken van functies die standaard werken met gevoelige of bijzondere privé (persoons) gegevens moeten worden uitgezonderd van geautomatiseerd veiligstellen. De landsadvocaat benoemt de volgende soort functies:
  - bedrijfsarts, -psycholoog, -fysiotherapeut, -verpleegkundige;
  - (leden van de) ondernemingsraad;
  - bedrijfsmaatschappelijk werkers en andere vertrouwenspersonen;
  - beveiligingsautoriteit;
  - personen met vertrouwensfuncties. Deze lijst is niet uitputtend, organisaties leggen vast welke functies hieronder vallen.
- Organisaties krijgen de mogelijkheid om na veiligstelling privé chats uit te zonderen.
- De toegang tot de gearchiveerde chatberichten is strikt beperkt tot de reikwijdte van één specifiek informatieverzoek en op verzoek van de eigenaar van de chatberichten.
- De verplichting om een regeling voor het doorzoeken van chatconversaties vast te stellen. Bij het opstellen van deze regeling, het doorzoekprotocol, dient rekening te worden gehouden met de uitgangspunten van dataminimalisatie en privacy by design & default (o.a. strikt autorisatie-, loggings-, en beveiligingsbeleid).
- Privé chatberichten die ten onrechte automatisch zijn gearchiveerd kunnen op verzoek worden verwijderd.
- Organisaties dienen voorafgaand aan het overbrengen van chatberichten naar een archiefinstelling de chatberichten te screenen op privé berichten en deze berichten vervolgens te verwijderen.
- Bij overbrengen van de chatberichten naar een archiefinstelling na te gaan of er beperkende bepalingen aan de openbaarheid moeten worden gesteld.
- Het opstellen van een privacyverklaring waarin duidelijk is verwoord hoe met persoonsgegevens wordt omgegaan en hoe de betrokkene gebruik kan maken van zijn rechten.
- Er zal onderzoek worden gedaan naar de mogelijkheid om onnodig automatisch gearchiveerde chatberichten te identificeren en uit te zonderen uit de afgezonderde omgeving, zowel vooraf als achteraf.
- Organisaties dienen de toepassing van de voorgestelde werkwijze te monitoren.

In de Rijksbrede DPIA is nog een aantal additionele maatregelen geformuleerd. In de bijlage *Privacymaatregelen* staat het overzicht hiervan (*te vinden in de beleidslijn archivering chatberichten*).

De belangrijkste privacymaatregelen voor organisaties zijn:

- Wanneer er op het zakelijk middel toch beperkt privé of partijpolitieke communicatie plaatsvindt, zorg er dan als organisatie voor dat de eigenaar van de chatgesprekken de zuiver privé en partijpolitieke chatberichten uit de eigen chatgesprekken kan verwijderen.
- Wanneer de berichteneigenaar de zuiver privé en partijpolitieke chatberichten niet uit de eigen chatgesprekken heeft verwijderd, komen de zuiver privé en partijpolitieke chatberichten niet in aanmerking voor openbaarmaking. Chatberichten die in het bericht zowel zakelijke als privé of partijpolitieke onderwerpen in zich dragen, mogen niet worden verwijderd. Deze vallen onder het organisatiearchief.
- Er moet een procedure worden ingericht om op verzoek chatgesprekken of berichten met bijzondere persoonsgegevens of personeelsvertrouwelijke gegevens te verwijderen dan wel te lakken.

Er zal moeten worden voorzien in (bindende en afdwingbare) regelingen voor de toegang tot de veiliggestelde e-mails en chatgesprekken. Ook moet het inzagerecht goed zijn geregeld door een strikt autorisatie- en loggingsbeleid, beveiligingsbeleid en doorzoekprotocol vast te stellen en te hanteren. In het doorzoekprotocol is duidelijk vastgelegd wie deze informatie op welke gronden kan raadplegen en hoe dit gebeurt. Toegang dient in ieder geval strikt beperkt te zijn tot de reikwijdte van het betreffende informatieverzoek.

5. Archivering en selectie

Archiveren is meer dan alleen het bewaren van informatie. Archiveren is het duurzaam toegankelijk maken en houden van overheidsinformatie, zodat deze nu en in de toekomst bruikbaar is voor iedereen die het recht heeft om de informatie in te zien. Niet alle overheidsinformatie hoeft (blijvend) te worden bewaard. In het kader van goed informatiebeheer is het ook nodig dat overheidsinformatie (op termijn) wordt vernietigd. Dit wordt bepaald op basis van waardering en selectie, waarmee je bepaalt welke overheidsinformatie bewaard blijft en welke niet.

Aggregatieniveaus van chatberichten

Bij chatberichten is het bericht binnen de chatconversatie het kleinste archiefbescheiden/document in de zin van de Archiefwet.
Bij de selectie van chatberichten wordt onderscheid gemaakt tussen drie aggregatieniveaus:

- Een chatbericht zelf is één technisch op zichzelf staand bericht, dat tevens het laagste aggregatieniveau van een document vormt volgens de documentdefinitie in de Archiefwet
- Een chatconversatie is een doorlopende communicatiestroom die in 1-op-1 of in groepsverband kan worden uitgewisseld. Een chatconversatie bevat de behandeling van een veelvoud aan chatgesprekken zonder dat er op een natuurlijke wijze een begin en een einde aan de conversatie zit, zoals bijvoorbeeld bij een beleidsnota wel het geval is.
- Een chatgesprek bestaat uit chatberichten, die begrensd zijn in tijd en in onderwerp.

Het is niet toegestaan om te vernietigen binnen een chatbericht, omdat je daarmee de authenticiteit van het documenten schaadt.

Belangrijke kanttekeningen:

- Zakelijke chatberichten worden in de context van chatconversaties met daarin zakelijke chatgesprekken bewaard. Het chatgesprek kan worden beschouwd als een aggregatie van meerdere berichten die een onderlinge samenhang vertonen en een begin en een einde kennen. Daarmee is het gesprek een geaggregeerd document onder de (nieuwe) Archiefwet. Alle zuiver privé en partijpolitieke chatberichten, die zich in een zakelijk chatgesprek bevinden, zijn echter geen documenten in de zin van de Archiefwet en mogen dus verwijderd worden uit het zakelijke gesprek, mits het chatgesprek als geheel daarmee nog wel begrijpelijk is. De verwijdering van deze berichten moet wel zichtbaar zijn als deel van het gesprek, inclusief meta-data die aangeeft wanneer dit is verwijderd. Hiermee borgen we de betrouwbaarheid en interpreteerbaarheid van het zakelijke chatgesprek.
- Vanuit het oogpunt van archivering zijn niet alleen de zakelijke chatberichten en chatgesprekken met daarbinnen de diverse informatieobjecten (tekst, audio, afbeeldingen) relevant, maar ook de metadata die belangrijke contextinformatie verschaft.

Selectielijst

Rijksoverheidsorganisaties bepalen in samenspraak met de Algemene Rijksarchivaris hoelang hun informatie bewaard moet worden. Hierbij moeten zij rekening houden met de Archiefwet en verschillende belangen waarvoor informatie gearchiveerd wordt. De Rijksarchivaris maakt modelselectiebesluiten voor de Rijksoverheid. Het Nationaal Archief heeft een modelselectielijst voor chatberichten opgesteld op basis van de Capstone-methodiek. Elke organisatie is verplicht een eigen aanvullende selectielijst vast te stellen (volgens het reguliere proces met betrokkenheid van de **externe** deskundige), inclusief een overzicht van de relevante sleutelfuncties. Op basis hiervan kunnen de chatberichten op termijn worden vernietigd dan wel overgebracht worden naar het Nationaal Archief. Zolang die lijst ontbreekt, mag er geen vernietiging van zakelijke chatberichten plaatsvinden.
Maatwerk (afwijken van de modelselectielijst opgesteld door het NA) is mogelijk, mits; er een eigen systeem- en risicoanalyse wordt uitgevoerd, en de maatwerk selectielijst wordt getoetst en akkoord bevonden door de externe deskundige én de Algemene Rijksarchivaris.

Selectie en waardering in de modelselectielijst

De zakelijke chatgesprekken en -berichten van ambtenaren die wel in de groep sleutelfuncties vallen en die een bewaartermijn van meer dan 1 jaar hebben: worden vanuit commerciële chatapps wel gemigreerd naar een centraal of door de organisatie beheerd systeem. De zakelijke chatgesprekken en -berichten van ambtenaren die niet in de groep sleutelfuncties vallen en die een relatief korte bewaartermijn van minder dan 1 jaar hebben:

- worden vanuit commerciële chatapps niet gemigreerd naar een centraal beheerd systeem, maar blijven beschikbaar op de telefoon van de ambtenaren tot de bewaartermijn, zoals vastgelegd in de selectielijst, is verstreken waarna vernietiging volgt.
- blijven bij zelf beheerde applicaties beschikbaar in de applicatie tot de bewaartermijn vastgelegd in de selectielijst is bereikt, waarna vernietiging volgt.

Uitzonderingen

Naast de eerder genoemde uitzonderingen (vertrouwensfuncties, PA's) zijn er ook contextgebonden uitzonderingssituaties:

- Publieke of organisatieaccounts: moeten worden gekoppeld aan zaaksystemen of apart opgenomen in de selectielijst. Communicatie met burgers of externe partijen wanneer deze al separaat benoemd zijn in de selectielijst van een organisatie. Denk hierbij aan processen als publieksvoorlichting.
- Hotspot-onderwerpen: in het geval van een hotspot maakt de organisatie voor de desbetreffende hotspot een sleutelfunctieoverzicht van de actoren die een belangrijke rol hebben gespeeld in de gebeurtenis, op basis waarvan vanaf het begin tot het moment van het afronden van de hotspot de archivering gaat plaatsvinden. Dit is echter een separaat proces.
- Buitenland: ook tijdens buitenlandse dienstreizen geldt de Archiefwet. Technische beperkingen moeten expliciet worden vastgelegd. Rijksoverheidsorganisaties kunnen eventueel afwijkend beleid hanteren bij buitenlandse dienstreizen en bij personeel dat in het buitenland werkt. Hierbij kan het voorkomen dat medewerkers tijdelijk vervangende mobiele middelen tot hun beschikking krijgen en/of gebruik moeten maken van afwijkende chatapplicaties. Zakelijke chatberichten vallen ook in deze gevallen onder de Archiefwet en moeten veiliggesteld worden. Als dit buitenproportioneel lastig is, moet door de organisatie geregistreerd worden dat dit niet mogelijk is. Departementen leggen deze uitzonderingen vast, als die ertoe leiden dat een deel van de zakelijke communicatie niet veiliggesteld kan worden.

Vernietiging

Met de vaststelling van bewaartermijnen in de organisatie of Rijksbrede selectielijst worden zorgdragers ook geacht de overheidsinformatie (de zakelijke chatberichten) te vernietigen.
Verwijdering van chatberichten is alleen toegestaan onder duidelijke voorwaarden:

- Privé- of partijpolitieke chatberichten binnen zakelijke gesprekken mogen verwijderd worden, mits dit gebeurt met zichtbare metadata.
- Bij een chatbericht dat zowel niet-zakelijke als zakelijke informatie bevat, weegt het overheidsbelang zwaarder. Het chatbericht in kwestie moet dan wel gearchiveerd worden.
- Privé- of partijpolitieke zinnen of zinsdelen binnen één zakelijk chatbericht mogen niet verwijderd worden.
- Zakelijke chatberichten worden vernietigd of overgebracht naar het Nationaal Archief, afhankelijk van de bewaartermijn.

De chatberichten van niet-sleutelfunctionarissen met een korte bewaartermijn van één jaar hoeven niet te worden veiliggesteld en blijven op de betreffende telefoon of het device staan. Hierdoor ontbreekt zicht op het tijdig en juist vernietigen van de berichten na verloop van de bewaartermijn. Om de vernietigingsprocedure uit artikel 8 van het Archiefbesluit uitvoerbaar te maken stelt de beleidslijn dat organisaties mogen afwijken van de in de modelselectielijst vastgestelde bewaartermijn van één jaar. Dit doen zij door in de door hun gebruikte chatapps bij Instellingen te kiezen voor de langst mogelijke termijn voor geautomatiseerde vernietiging. Vanaf het moment dat een nieuwe termijn in de instellingen voor geautomatiseerde vernietiging beschikbaar komt, welke dichterbij de bewaartermijn van de selectielijst ligt, zal die instelling moeten worden gehanteerd. Belangrijk is dat de keuzen voor afwijking duidelijk wordt gecommuniceerd naar burgers, journalisten en andere partijen. Voor implementatie dienen rijksoverheidsorganisaties onderling afspraken te maken over het al dan niet inzetten van geautomatiseerde vernietiging, omdat dit kan leiden tot verschillen in bewaartermijnen tussen organisaties.

6. Verwante regels en eisen aan implementatie

Tot slot beschrijft de beleidslijn de verschillende gerelateerde regels op gebied van geautomatiseerde chatarchivering. Hieronder volgt een kort overzicht van de verschillende typen regels Voor de complete uitwerking wordt naar de tekst van de vastgestelde beleidslijn verwezen. Het betreft regels voor:

- Het gebruik van chatapplicaties en welke er voor zakelijk gebruik geselecteerd mogen worden
- communicatiebeleid voor zakelijke chats
- archiveringstechniek
- duurzame toegankelijkheid
- migratie
- metadata
- beschikbaarheid van chat berichten
- controle en monitoring

Uit deze regels volgen een aantal eisen en verplichtingen, die staan hieronder opgesomd.

Eisen aan implementatie

- Defensie- en Rijksambtenaren en bewindspersonen ontvangen zakelijke middelen om taakgericht te communiceren.
- Er moet een procedure zijn ingericht om op verzoek personeelsvertrouwelijke en bijzondere persoonsgegevens in chatgesprekken te kunnen uitzonderen c.q. markeren.
- Het is noodzakelijk:
  - zorg te dragen voor bindende en afdwingbare regelingen voor opslag en toegang tot informatie te hebben vastgelegd, waarbij de beginselen van dataminimalisatie en privacy by design als uitgangspunt zijn genomen, inclusief strikt autorisatie-, loggings, beveiligingsbeleid en doorzoekprotocol.
  - een waarschuwingsfunctie in de chatapplicatie in te regelen, die aan de betreffende persoon kenbaar maakt dat zijn of haar chatgesprekken (binnen een aantal dagen) zullen worden veiliggesteld c.q. gearchiveerd;
  - de noodzakelijke beveiligingsmaatregelen, zoals bijvoorbeeld versleutelde opslag ter voorkoming van datalekken, ingeregeld te hebben.
  - Het gevolgde proces voor migratie wordt vastgelegd via een migratiebesluit. Op deze wijzen wordt er verantwoording afgelegd. Een specificatie van de specifieke berichten die zijn gemigreerd zijn niet nodig, wel in algemenere termen.
  - Stel als organisatie/zorgdrager een migratiebesluit op waarin is aangegeven op welke wijze de gestelde eisen op het gebied van informatiehuishouding, informatiebeveiliging en privacy ten aanzien van de geordende en toegankelijke staat wordt voldaan en welk proces hiervoor is ingericht. Dit is een éénmalige actie voor het vastleggen van de beschrijving van het archiefproces.
  - De eisen aan (de inhoud van) het document en de minimale set aan metadata die bewaard moeten blijven, worden door het Nationaal Archief voorgeschreven en zijn terug te vinden in het informatieblad ‘archiveren chatberichten’. Wanneer een organisatie meer metadata, die te categoriseren zijn als persoonsgegevens, wil opslaan, dan moet zij dit ook kunnen verantwoorden, onder meer via een eigen aanvullende DPIA. In deze DPIA moet de keuze tot verwerking van de additionele metadata/persoonsgegevens zijn opgenomen en onderbouwd.
  - Organisaties dienen voor het mogen doorzoeken van de veiliggestelde chatgesprekken een aparte regeling vast te stellen. In deze regeling dient in ieder geval te zijn opgenomen:
    - aan welke voorwaarden een informatieverzoek moet voldoen;
    - wie beslissingsbevoegd is voor het (laten) uitvoeren van een onderzoek;
    - hoe, door wie en met welke hulpmiddelen het onderzoek wordt uitgevoerd.
    - welke eisen (op het gebied van kennis en kunde, gedrag en niveau van veiligheidsonderzoek)
    - aan die personen worden gesteld.
    - hoe om te gaan met privé, partijpolitieke of personeelsvertrouwelijke berichten die worden aangetroffen of berichten die (bijzondere) persoonsgegevens bevatten.

  - Toegang tot de veiliggestelde chatgesprekken is daarnaast strikt beperkt tot de reikwijdte van één specifiek informatieverzoek.
  - Rijksdienstorganisaties bouwen voldoende controles en verplichte audits in het informatiebeheer in om aan te kunnen tonen dat het archief- en informatiebeheerbeleid aantoonbaar wordt nageleefd. Dit doen zij door jaarlijks opzet, bestaan en werking van de risico- of procesbeheersing van chatberichtenarchivering binnen de organisatie te controleren. De bevindingen worden gedeeld met het bestuur, management en CIO Rijk
- Zakelijke chatgesprekken worden veilig (conform BIO) en voorzien van waarborgen opgeslagen, zodat:
  - alleen bevoegden hier (tijdelijk) toegang toe hebben,
  - ongeautoriseerde toegang (een inbreuk op vertrouwelijkheid/exclusiviteit) wordt voorkomen,
  - continuïteit (beschikbaarheid) geborgd wordt,
  - inbreuken op integriteit (zoals kunnen wijzigen of wissen) worden voorkomen,
  - verantwoording mogelijk is.

Elke organisatie communiceert richting haar medewerkers welke vorm en typen berichtenapps voor zakelijk gebruik zijn toegestaan. Ook richt elke organisatie een proces en voorzieningen voor archivering in voor informatie die de organisatie verstuurt of ontvangt via de desbetreffende berichtenapps. Rijksdienstorganisaties maken daarbij gebruik van de kaders en eisen die vanuit CIO Rijk worden gesteld.

Verplichte evaluatie

Om de effecten van de Capstone-methodiek op gegevensbescherming te evalueren, worden periodieke evaluatiemomenten en audits verricht met ten minste de volgende departementale controles:

Bewustwording en gedrag
Controleer of:
- Nieuwe rijksmedewerkers tijdens hun on-boarding over de bestaande handleidingen en gedragsinstructies over het gebruik van chatapplicaties en het scheiden van zakelijk en privé worden geïnformeerd.
- Voorlichting met speciale aandacht voor de omgang met gevoelige en bijzondere overheidsinformatie structureel plaatsvindt.
- Scheiding van zakelijke en privé communicatiestromen in gedrag is bestendigd. De mate waarin handmatige selectie nog moet plaatsvinden is hier een indicator voor.

Bestaan
- Controleer het bestaan, de kwaliteit en actualiteit van de documentatie waaronder procesbeschrijvingen, procedures en instructies.
- Controleer of regels of beleid, dat duidelijk afbakent welke afdelingen, functies of categorieën van personen niet hoeven te worden meegenomen in de archivering, aanwezig en up-to-date zijn.
- Controleer of departementale handleidingen en gedragsinstructies te vinden zijn voor alle overheidsmedewerkers

Werking
- De werking wordt gecontroleerd via steekproeven op:
  - de samenstelling en volledigheid van de gearchiveerde chatgesprekken.
  - de aanwezigheid van gearchiveerde chatgesprekken van een aantal sleutelfuncties.
  - de audit-trail, logging en monitoring van toegang tot het chatarchief.
  - De aanwezigheid van gevoelige gegevens of bijzondere persoonsgegevens.
  - De instelling van geautomatiseerde vernietiging in chats binnen de gebruikte chatapplicaties (mits de organisatie hiervoor gekozen heeft).

- Controleer periodiek:
  - of bewaartermijnen van chatberichten met een maximaal bewaartermijn worden gehonoreerd . c.q. vernietiging daadwerkelijk heeft plaatsgevonden. Hiermee wordt gecontroleerd dat gegevens niet langer worden bewaard dan noodzakelijk, wat bijdraagt aan de dataminimalisatie
  - Of de zakelijke chatberichten van de functies die zijn uitgezonderd van het geautomatiseerd veiligstellen van chatgesprekken overeenkomstig de Capstone-methodiek wel handmatig worden veiliggesteld.

Randvoorwaarden voor succes

Op beleidsniveau gelden daarnaast de volgende uitgangspunten:

- Archivering vindt zoveel mogelijk geautomatiseerd plaats via de Capstone-methodiek (op basis van sleutelfuncties).
- Organisaties zijn zelf verantwoordelijk voor naleving, monitoring, en interne audits.
- Chatgebruik voor gerubriceerde of vertrouwelijke informatie via commerciële apps wordt actief ontmoedigd.
- Alleen bevoegde medewerkers mogen, onder strikte voorwaarden, toegang krijgen tot veiliggestelde berichten.

Organisaties mogen nadere gedragsregels opstellen, mits deze binnen de centrale rijkskaders passen.

Maatregelen noodzakelijk voor implementatie

Hieronder volgt een lijst met noodzakelijke maatregelen benodigd voor
een succesvolle implementatie:
Op basis van de eind 2023 ontwikkelde en in 2024 aangescherpte model selectielijst voor chatgesprekken wordt per zorgdrager een eigen selectielijst inclusief een sleutelfunctieoverzicht op- en vastgesteld. Waar wenselijk wordt dit centraal gefaciliteerd via een mandaatbesluit.
Per oganisatie c.q. zorgdrager wordt in ieder geval onderzocht of:

- de Rijksbrede lijn voor het sleutelfunctieoverzicht een aanvulling behoeft;
- de Rijksbrede lijst met categorisch uitgezonderde functies voor het desbetreffende departement aanvulling behoeft.

Voordat een Rijksoverheidsorganisatie daadwerkelijk overgaat op het onder beheer brengen en archiveren van chatgesprekken is het verplicht om na te gaan of er een additionele DPIA moet worden uitgevoerd. Dit is het geval wanneer organisaties besluiten om meer meta-data, die te categoriseren zijn als persoonsgegevens, op te slaan, dan de set meta-data die in de Rijksbrede DPIA zijn opgenomen.
Bewindspersonen en ambtenaren (sleutelfuncties en niet-sleutelfuncties) moeten worden geïnformeerd over de beleidslijn en daaruit voortvloeiende werkprocessen, gedragsregels en overige instructies. Hiervoor is het noodzakelijk om alle medewerkers hierover tijdig te informeren inclusief het moment van ingebruikname van de chatarchivering bij een organisatie, zodat medewerkers daar hun gedrag op kunnen aanpassen.

Beheer beleidslijn

Het eigenaarschap van de beleidslijn chatberichtenarchivering ligt bij CIO Rijk. Dit geldt ook voor het beheer ervan.

Dit document is een samenvatting gebaseerd op de volledige tekst van de beleidslijn, welke is vastgesteld. Het uitgebreide naslagwerk is te vinden op: xxx

Evaluatie

Drie jaar na invoering vindt een brede evaluatie plaats door CIO-Rijk vanuit het C-stelsel van de werking en effecten van het beleid.

Deze brochure is een uitgave van:

Rijksoverheid
Postbus 00000 | 2500 AA Den Haag
T 0900 654 32 10 (ma t/m vrij 9.00 – 21.00 uur)

Ontwerp: **OSAGE, Utrecht**

Mei 2026