Module 2 Beleid en wettelijke kaders

De wettelijke kaders

Overheidsinformatie in chatapplicaties valt onder de Archiefwet. Daarnaast heeft andere wet- en regelgeving ook invloed op het archiveren van deze informatie., zoals de Algemene verordening gegevensbescherming (AVG) die over de privacy waakt. Deze module licht toe wat de voornaamste wet- en regelgeving is die van toepassing is op dit onderwerp. Ook vat de module samen hoe je de belangrijkste bepalingen met deze handreiking kunt toepassen.

A. Archiefwet;
   De Archiefwet 1995 wordt gemoderniseerd. De nieuwe Archiefwet treedt naar verwachting in 2027 op 1 januari 2027 in werking. De Archiefwet 1995 (Archiefwet) regelt het beheer van en de toegang tot overheidsarchieven.
   De Archiefwet hanteert in artikel 1 de volgende definitie voor archiefbescheiden: 'bescheiden, ongeacht hun vorm, door de overheidsorganen ontvangen of opgemaakt en naar hun aard bestemd daaronder te berusten'. Overheidsinformatie is alle vastgelegde informatie die de overheid ontvangt, verwerkt of maakt bij het uitvoeren van haar taken. Hierbij wordt geen onderscheid gemaakt in de (technische) vorm, zoals e-mail, websites, die de informatie heeft of de plaats waar de informatie bewaard wordt. Chatberichten vallen ook onder deze definitie en dus onder de toepassing van de Archiefwet. Dit omvat zowel het profiel, de berichten als de reacties op deze berichten. En alle eventuele wijzigingen en de metadata. Dit speelt een rol bij het bepalen van de archiveringsmethode en -frequentie.

   Het Archiefbesluit 1995 (Archiefbesluit) wijst in artikel 2 op 'het belang van de in de archiefbescheiden voorkomende gegevens voor overheidsorganen, voor recht- of bewijszoekenden en voor historisch onderzoek'. Daarom legt de Archiefwet in artikel 3 overheidsorganen de verplichting op om '[…] de onder hen berustende archiefbescheiden in goede, geordende en toegankelijke staat te brengen en te bewaren'. Een overheidsorganisatie mag zelf invullen hoe het aan deze wettelijke verplichtingen voldoet. Bij voorkeur voordat of vanaf het moment de organisatie gebruikmaakt van een systeem. Dat noemen we archiveren by design.
   Verder bepaalt de Archiefwet in artikel 5 dat overheidsorganen 'selectielijsten' moeten ontwerpen 'waarin tenminste wordt aangegeven welke archiefbescheiden voor vernietiging in aanmerking komen'. Artikel 5 van het Archiefbesluit 1995 licht toe dat selectielijsten moeten verduidelijken of 'de archiefbescheiden bewaard worden dan wel na welke termijn zij voor vernietiging in aanmerking komen'. Dat geldt dus ook voor chatberichten.
   Artikel 3 van de Archiefwet verplicht overheidsorganen 'zorg te dragen voor de vernietiging van de daarvoor in aanmerking komende archiefbescheiden'. En artikel 12 om 'de archiefbescheiden die niet voor vernietiging in aanmerking komen en ouder zijn dan twintig jaar over te brengen naar een archiefbewaarplaats'. Bij het overbrengen van overheidsinformatie naar een archiefbewaarplaats geldt het uitgangspunt in artikel 14 van de Archiefwet dat deze informatie openbaar is. Wel kunnen volgens artikel 15 van de Archiefwet 'beperkingen aan de openbaarheid voor een bepaalde termijn' gesteld worden. Daarvoor kent de Archiefwet drie uitzonderingsgronden. Een voorbeeld is de eerbiediging van de persoonlijke levenssfeer. Dat geldt ook voor blijvend te bewaren chatberichten.
   Meer informatie over de Archiefwet is te vinden op de websites van de Rijksoverheid en de Vereniging van Nederlandse Gemeenten.

   NB. De Afdeling bestuursrechtspraak van de Raad van State (Raad van State) heeft als hoogste bestuursrechter in 2019 uitgesproken dat WhatsApp- en sms-berichten (chatberichten) documenten in de zin van de Wet openbaarheid van bestuur (Wob) zijn en dus onder een Wob-verzoek kunnen vallen. Het betrof de uitspraak: 201800258/1/A3, ECLI:NL:RVS:2019:899. Op 21 oktober 2020 heeft de Raad van State een nieuwe uitspraak

gedaan, deze keer over eventuele bewaarplichten voor WhatsApp- en sms-berichten. Het gaat om uitspraak 201905713/1/A3, ECLI:NL:RVS:2020:2477.

B. Wet Open overheid;
De Wet open overheid (Woo) regelt het recht van burgers op overheidsinformatie.

De Woo hanteert in artikel 2.1 de volgende definitie voor publieke informatie: 'Informatie neergelegd in documenten die berusten bij een orgaan, persoon of college'. En de volgende definitie voor document: 'Een door een orgaan, persoon of college […] opgemaakt of ontvangen schriftelijk stuk of ander geheel van vastgelegde gegevens dat naar zijn aard verband houdt met de publieke taak van dat orgaan, die persoon of dat college'. Chatberichten vallen ook onder deze definitie en dus onder de toepassing van de Woo.

De Woo stelt in artikel 1.1 het volgende: 'Eenieder heeft recht op toegang tot publieke informatie zonder daartoe een belang te hoeven stellen, behoudens bij deze wet gestelde beperkingen'. De Woo verplicht in artikel 3.1 overheidsorganisaties zoveel mogelijk informatie open te stellen voor iedereen. Dit is actieve openbaarmaking. Daarnaast stelt artikel 4.1 dat iedereen informatie mag vragen over wat de overheid doet. Dit is passieve openbaarmaking. Chatberichten kunnen dus actief openbaar worden gemaakt en kunnen betrokken worden bij een Woo-verzoek. Wel bepaalt artikel 5.1 van de Woo dat er uitzonderingen mogelijk zijn op het openbaar maken van informatie. Daarvoor voorziet de Woo vijf absolute en negen relatieve uitzonderingsgronden. Een voorbeeld van een absolute uitzonderingsgrond zijn bepaalde persoonsgegevens zoals ras of etnische afkomst. Een voorbeeld van een relatieve uitzonderingsgrond is de bescherming van de persoonlijke levenssfeer, zoals adresgegevens.[1]

Tot slot legt de Woo in artikel 2.4 overheidsorganisaties de volgende algemene verplichting op met betrekking tot overheidsinformatie: 'Een bestuursorgaan draagt er zorg voor dat de documenten die het ontvangt, vervaardigt of anderszins onder zich heeft, zich in goede, geordende en toegankelijke staat bevinden'. Een overheidsorganisatie mag zelf invullen hoe het aan deze wettelijke verplichtingen voldoet.

C. AVG;
De Algemene verordening gegevensbescherming (AVG) is een Europese verordening die de regels voor het verwerken van persoonsgegevens door overheidsinstanties en bedrijven in de hele Europese Unie (E.U.) standaardiseert. Verwerken van persoonsgegevens houdt dus in: alles wat een organisatie kan doen met die gegevens.

De AVG hanteert in artikel 4 de volgende definitie van persoonsgegevens: 'Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon'. En stelt in artikel 9 dat er naast 'gewone' ook 'bijzondere' persoonsgegevens zijn. Bijzondere persoonsgegevens zijn gegevens die zó privacygevoelig zijn dat het grote(re) impact op iemand kan hebben als deze gegevens worden verwerkt. Hierbij gaat het gaat om persoonsgegevens zoals over ras of etnische afkomst, politieke opvattingen, Daarom is de verwerking van bijzondere persoonsgegevens verboden, tenzij een in de AVG genoemde uitzondering van toepassing is. Chatberichten vallen onder de toepassing van de AVG, aangezien o.a. ook namen en herleidbare telefoonnummers onder de AVG vallen en er ook in de inhoud van chatgesprekken persoonsgegevenskunnen voorkomen.
Artikel 4 van de AVG geeft ook aan dat 'verwerking' betrekking heeft op een breed scala aan verschillende verwerkingen van persoonsgegevens. Die zowel handmatig als geautomatiseerd kunnen zijn. Doorgaans zijn dat voor overheidsorganisaties verwerkingen die:

- voldoen aan een wettelijke verplichting die op de gegevensverwerkende overheidsorganisatie rust (artikel 6 lid 1 onder c van de AVG) en/of

[1] wetten.nl - Regeling - Wet open overheid - BWBR0045754

- een taak van algemeen belang vervullen. Of een taak vervullen voor de het openbaar gezag dat de verwerkende organisatie uitoefent (artikel 6 lid 1 onder e van de AVG).

Artikel 5 van de AVG kent een aantal 'beginselen inzake de verwerking van persoonsgegevens'. Het stelt onder andere dat persoonsgegevens verwerkt moeten worden op een 'wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is'. Overheidsorganisaties hebben een gegronde reden mandaat nodig om persoonsgegevens rechtmatig te kunnen verzamelen en beheren. Een ander belangrijk beginsel is 'doelbinding'. Organisaties mogen persoonsgegevens alleen verzamelen voor een gerechtvaardigd doel. Dat doel moet specifiek zijn en vooraf uitdrukkelijk zijn omschreven. Verder geldt ook het principe van 'minimale gegevensverwerking' (of 'dataminimalisatie'). De verwerking van de gegevens moet passen bij het doel. En de organisatie mag niet meer gegevens verwerken dan noodzakelijk om het doel te bereiken.
Doelbinding houdt ook in dat de organisatie de gegevens niet ineens voor een heel ander doel mag gebruiken. Artikel 89 van de AVG verduidelijkt dat 'verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden' een verdere gegevensverwerking is; het doel is verenigbaar met het oorspronkelijke verwerkingsdoel. Het archiveren van chatberichten volgens de Archiefwet is zo'n verdere verwerking. Wel moeten er volgens datzelfde artikel 89 'passende waarborgen' zijn om het beginsel van minimale gegevensverwerking te garanderen. Denk aan pseudonimiseren (het omzetten van persoonsgegevens naar een niet-herleidbare code). En/of andere organisatorische en technische maatregelen, zoals de beperking van de toegang tot informatie. Anonimiseren is geen optie. Dit leidt tot onomkeerbaar verlies van historisch waardevolle informatie.

Artikel 17 verduidelijkt ook dat dit recht in principe niet geldt bij het voldoen aan een wettelijke verplichting en/of bij het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag. En bij het daarop aansluitende archiveren in het algemeen belang. Dat laatste slaat op blijvend te bewaren overheidsinformatie die nog naar een archiefbewaarplaats overgebracht moeten worden. En op overheidsinformatie die al overgebracht is.
Tot slot kent de AVG een aantal privacy-rechten toe aan individuen.

D. Digital Markets Act;
De Digital Markets Act (DMA) bevat regels speciaal voor zeer grote platforms zoals zoekmachines, webbrowsers, besturingssystemen en social media. Zij worden 'poortwachters' genoemd. De Europese Commissie heeft aangewezen welke online bedrijven dit zijn.
Poortwachters hebben zo'n grote rol op de online markt, dat ze zich aan de extra regels uit de DMA moeten houden. Zo zorgt de DMA voor eerlijke voorwaarden voor consumenten en zakelijke gebruikers. En voor ruimte voor alternatieve platforms.
De DMA bevat regels om mensen en bedrijven minder afhankelijk te laten zijn van poortwachters. Iedereen moet vrij kunnen kiezen tussen diensten van een platform en die van kleinere concurrenten. Poortwachters mogen gebruikers bijvoorbeeld niet verplichten om een bepaalde betaaldienst te gebruiken.

Voor de archivering van chatberichten is van belang dat de chatapplicaties van o.a. META -, WhatsApp en Facebook - messenger, deel uitmaken van deze regeling. Dit betekent dat hiervoor naar specifieke regels wordt gekeken waar deze aan moeten voldoen, zoals de toegang vanuit andere chatapplicaties. Oftewel het kan verplicht worden gesteld dat met gebruikers van Whats-Aapp ook vanuit een andere chatapp berichten kunnen worden gestuurd en vice versa. Dit kan de keuze voor de archiveringstrategie en beleid beïnvloeden. Het opent meer mogelijkheden dan er op dit moment zijn, waarbij er geen/ beperkt toegang (toegang van wat?) mogelijk is.

E. Cyberbeveiligingswet
De Cyberbeveiligingswet (Cbw) is de Nederlandse omzetting van de Europese Network and

Information Security directive, of NIS2-richtlijn. De NIS2-richtlijn is gericht op het verbeteren van de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten. Deze verbetering is noodzakelijk vanwege meer afhankelijkheid van digitalisering en toegenomen dreigingen.
Organisaties die onder de Cyberbeveiligingswet (Cbw) vallen hebben een zorgplicht. Dit betekent dat ze passende maatregelen moeten nemen om de continuïteit van hun diensten zoveel mogelijk te waarborgen en de informatie die ze gebruiken, te beschermen. Dat doen organisaties op basis van een risicobeoordeling. De maatregelen voor de zorgplicht worden nader uitgewerkt in de Cyberbeveiligingswet en de lagere regelgeving.
Nadere invulling van de zorgplicht voor de overheid zal gebeuren via de Baseline Informatiebeveiliging Overheid (BIO)2.

De BIO2 is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De BIO2 weerspiegelt de internationale beveiligingsnormen (NEN-EN-ISO/IEC 27001:2023 (nl) en NEN-EN-ISO/IEC 27002:2022 (nl)) en vraagt om een risicogerichte benadering. Hiermee kunnen overheidsinstanties maatregelen afstemmen op specifieke risico's. Bij het gebruik van chatapplicaties en de archivering van chatberichten, die verschillende niveaus van informatie kunnen bevatten, afhankelijk van het beleid en gebruik moet de BIO ingezet worden om de risico's bij het gebruik van deze applicaties te beoordelen.

F. Sectorale Wetgeving
Sectorale wetgeving kan ook van toepassing zijn. In een aantal situaties zal sectorale wetgeving nadere eisen stellen aan de omgang met informatie, zowel over beheer als beveiliging als ook specifieke bewaartermijnen. Denk bijvoorbeeld aan de wet Politiegegevens. Kijk als organisatie altijd goed naar de eigen sectorale wetgeving of die eisen stelt zoals hier aangegeven en neem dat mee in de ontwikkeling van het beleid en de nodige beheersmaatregelen.

Beleid en regels

Een organisatie stelt op basis van de het wettelijke kader stelt een organisatiebeleid op. Hier wordt rekening gehouden met de wettelijke kaders en diens specifieke organisatie-omstandigheden. Dit hoofdstuk beschrijft de stappen om tot beleid te komen.

A. Beleid

Het beleid kent een aantal componenten. Het gaat over de keuze voor welke applicatie(s) er gebruikt kunnen worden. Over hoe er gebruik van mag worden gemaakt, over opslag en beheer van berichten, over privacy, informatiebeveiliging en over de methode van waarderen en selecteren.

Stap 1. Passend beleid
Het wettelijk kader geeft ruimte om zelf beleid te maken. Er zijn keuzes die gemaakt moeten worden die allemaal impact hebben op wat mogelijk en haalbaar is. Begin met het bepalen van het doel en de uitgangspunten voor de organisatie. Voor de Rijksoverheid verzorgt CIO Rijk het chatbeleid, waarbinnen nog individueel aanvullend beleid mogelijk is.

Voorbeeld doel (Uit het Rijksbrede beleid):
Het einddoel is om via heldere afspraken in deze beleidslijn duurzaam toegankelijke chatberichtenarchivering te kunnen realiseren voor de Rijksdienst in lijn met de eisen van de Archiefwet, Algemene Verordening Gegevensbescherming en Wet open overheid.

Hierbij horen een aantal uitgangspunten, (deels) gebaseerd op het wettelijke kader dat je wil toepassen.

Voorbeeld uitgangspunt: *Er wordt gebruik gemaakt van een telefoon en zakelijk nummer van de organisatie.*
Het doel en de uitgangspunten zijn het houvast bij het maken van keuzes en zorgen ervoor dat deze uitlegbaar en passend zijn voor de organisatie.

Stap 2. Heb zicht op het gebruik van chat

a. Overzicht maken

Maak een overzicht van alle chatapps en applicaties met chatfunctionaliteit die in de organisatie in gebruik zijn. Maak hiervoor gebruik van het algemene systeemoverzicht en vraag aan de systeemverantwoordelijke naar een eventuele chatfunctie. Voor de generieke chatapplicaties die in gebruik zijn, zet hiervoor een korte vragenlijst uit en /of interview medewerkers.
Valideer het overzicht dat is ontstaan binnen de organisatie. Het gaat er bij dit overzicht niet om zo volledig mogelijk te zijn, maar om de belangrijkste informatiestromen in kaart brengen. Zodat je het beleid goed vorm kan geven. Werk hiervoor ook samen met andere belanghebbende partijen zoals de privacy officer en informatiebeveiliging.
Beschrijf de verschillende applicaties en hun gebruik (voor zover bekend). Aan de hand van deze informatie kun je als organisatie afspraken maken over het gebruik, maar ook apps of functies blokkeren die niet gewenst zijn. Het helpt zo om aan het doel te voldoen dat met het beleid gerealiseerd moet worden.

b. Gebruik van chatapps

Er moeten afspraken gemaakt worden over welke chatapps medewerkers mogen gebruiken, voor welke doeleinden en waarvoor juist niet. wat wel of niet via chatapps gecommuniceerd mag worden. Dit is niet enkel een zaak van archivering en vraagt daarom afstemming met andere stakeholders, zoals het CIO office of de afdeling communicatie.

i. Keuze voor chatapps

Als organisatie moet bepaald worden welke chatapps en zakelijke applicaties met chatfuncties gebruikt mogen worden. En voor welke doeleinden.

1. Voorbeeld: een organisatie gebruikt blackberry messenger voor onderlinge communicatie, maar voor communicatie met andere partijen wordt whatsapp gebruikt.

Neem in de overwegingen mee het gemak waarmee de informatie gearchiveerd of vernietigd kan worden.

ii. Afspraken gebruik

Duidelijke afspraken zijn nodig. Stel afspraken op over het gebruik van chat in de applicatie. Een voorbeeld zijn de gedragsregels voor de digitale werkomgeving van de Rijksoverheid (Voorbeeld in kader volgt). Bij meerdere apps kunnen er afspraken gemaakt worden welke informatie in welke app gedeeld mag worden, of juist zeker niet. Denk hierbij aan afspraken over:

1. Zakelijk en privégebruik van de applicatie.
2. Het delen van gevoelige informatie
3. Delen van persoonsinformatie, bijv. ziektemelding via de chat.
4. Delen van bijlagen, zoals documenten
5. Afspraken of accordering over de app.

NB. Een voorbeeld van een regel is: *App met beleid niet over beleid.*

iii. Praktijk

Stap 3 . Neem privacy- en beveiligingsaspecten op

1) Privacy

Bij het gebruik van apps worden altijd persoonsgegevens gedeeld, in ieder geval zowel de

gegevens van de verzender en de ontvanger. Ook in de chatconversatie zelf. Dat betekent dat hier zorgvuldig mee moet worden omgegaan. Juist ook bij de opslag en archivering van chatberichten. Het beleid dient te beschrijven welke persoonsgegevens verwerkt worden in de chatapp(s) die onder het beleid vallen en hoe de privacy geborgd wordt. Hier hoort dan ook het opstellen van een Data Protection Impact Assessment (DPIA) bij. In een DPIA moet het volgende worden opgenomen:

- Een systematische beschrijving van de gegevensverwerking die de organisatie van plan is en de doeleinden hiervan.
- Een beoordeling van de noodzaak en de proportionaliteit van de verwerking. Een beoordeling van de privacyrisico's voor de mensen van wie je als organisatie de gegevens wilt verwerken.
- De beoogde maatregelen om (1) de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen) en (2) aan te tonen dat u aan de AVG voldoet.
  Een voorbeeld hoe dit vorm kan worden gegeven is het Afwegingskader Chat van de Rijksoverheid waarin het gaat over welke berichten Privé, partijpolitiek of personeelsvertrouwelijk zijn en welke zakelijk.

  NB. Voor het Rijksbeleid Chatarchivering is al een DPIA gemaakt. Organisaties die hieraan gebonden zijn hoeven dus niet zelf een DPIA uit te voeren, tenzij zij willen afwijken van het Rijksbrede beleid.

2) Beveiliging

a) End to end encryptie

Chatapps maken over het algemeen gebruikt om snel en veilig informatie uit te wisselen met gebruik van end-to-end-encryptie. End-to-end-encryptie (*end-to-end encryption* (E2EE), ook end-to-end-versleuteling of begin-tot-eindversleuteling) is het versleutelen van berichten op een zodanige wijze dat alleen de zender en ontvanger de inhoud van berichten kunnen lezen. Hiervoor wordt gebruik gemaakt van een protocol. Een protocol dat in gebruik is door verschillende applicaties zoals Signal, WhatsApp en Facebook Messenger is Signal Protocol. Dit protocol gebruikt verschillende technieken om een E2EE-verbinding mogelijk te maken waaronder het Double Ratchet-algoritme, elliptische curve Diffie-Hellman (ECDH) en AES-256.
End-to-end encryptie is veilig, hoewel er al wel mogelijkheden zijn om deze te omzeilen en toch met berichten mee te lezen. Dit is uit perspectief van privacy en informatiebeveiliging onwenselijk. Echter voor archivering is het juist wel nodig dat de organisatie toegang heeft tot de berichten. Deze moeten door de organisatie in beheer kunnen worden genomen. Bij de archivering moet de encryptie dus ook worden verwijderd.

b) Nieuwe functies in Chatapplicaties (WhatsApp)

Bij het gebruik van chatapplicaties bedoeld voor consumenten loop je een risico. Bij de afname van een consumentenproduct heb je als organisatie als regel geen controle over welke functies worden aangeboden. En vaak ook niet over de eigen zakelijke informatie. Het beheer ligt bij de aanbieder en de communicatie gaat over de servers van deze organisatie. Je moet als organisatie overwegen of je dit acceptabel vindt.

Voorbeeld: Een nieuwe ontwikkeling is het aanbieden van Generatieve AI in WhatsApp. Bij het gebruik van de AI-functie kan Meta beperkt in het appverkeer en deze informatie gebruiken om het AI-model verder te trainen. Deze functie is door Meta geïntroduceerd vanuit hun belang, als organisatie heb je hierin geen inspraak. Net zoals bij punt b, betrek hier alle stakeholders van de organisatie.

c) Opslag

De keuze hier is voor opslag op eigen servers (al dan niet een eigen cloudomgeving) of gebruik te maken van de door de leverancier gebruikte cloudopslag. Volg hiervoor het informatiebeveiligingsbeleid van de organisatie (gebaseerd op NIS2). En kijk ook naar het cloudbeleid van de organisatie zelf of voor de overheidslaag. Afhankelijk van de informatie die via de app gedeeld moet een keuze worden gemaakt. Er komt nieuw cloudbeleid voor de gehele overheid. Dit betekent dat vanaf dan er minder vrijheid is voor de eigen organisatie.

NB. Over het algemeen geldt dat een eigen omgeving voor de opslag van de informatie de meeste veiligheid biedt. Dit geniet de voorkeur.

Stap 4) Bepaal de waardering en selectiemethodiek

Tenslotte moet bepaald worden hoe de informatie uit de chatapplicaties gewaardeerd en geselecteerd wordt. Dit betekent een keuze voor een bepaalde methodiek. Hierbij is er de keuze tussen het gebruik van de sleutelfunctiemethodiek of de procesgerichte aanpak.

1) De sleutelfunctiemethodiek is de Nederlandstalige term voor de Capstone-methode. Deze door de National Archives and Records Administration (NARA) in de VS ontwikkelde methode is gebaseerd op het uitgangspunt dat sleutelfuncties zogenoemde informatieknooppunten 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. Daarmee wordt ook het toekomstig (historisch) onderzoek geborgd.
   Dit is in lijn met de vormvrijheid van selectielijsten die beschreven wordt in de Nota van Toelichting bij het Archiefbesluit: selectielijsten kunnen ingedeeld worden naar onder andere informatiestromen. Waar zowel e-mail, als chatberichten, een voorbeeld van zijn.
   In feite betekent de sleutelfunctie methodiek sleutelfunctie methodiek dat context toegekend wordt op basis van functie, in plaats van werkproces.
2) Procesgerichte aanpak. Bij een selectielijst gebaseerd op de werkprocessen van de organisatie (de bestaande selectielijst) moeten alle berichten op basis van de werkprocessen worden geselecteerd. Context en waardering wordt dus toegekend op basis van het werkproces.

NB. Zie Module W&S voor meer informatie.

Voorbeeld beleid: Beleidslijn Archivering Chatberichten Rijksoverheid. In de beleidslijn staan afspraken en (gedrags)regels rond het gebruik van berichtenapps en archivering van chatberichten en -gesprekken voor de rijksoverheid. Het biedt richtlijnen en toelichting.