Handreiking voor **ambtelijke organisatie**

Onder beheer brengen van e-mail, chatberichten en sociale media van **bewindspersonen**

Inhoudsopgave

1. Inleiding

Op de juiste manier omgaan met informatie zorgt voor transparantie, verantwoording en efficiëntie. Een goede informatiehuishouding helpt de overheid gegevens beter te beheren en te delen en is daarmee een belangrijke component voor het reconstrueren van (totstandkoming van) beleid. De huidige wetgeving vraagt hier ook om.
Een belangrijke stap daarin is het veiligstellen en onder beheer brengen van zakelijke informatie.[1] Bij informatieverlies is het voor overheidsorganisaties en hun medewerkers niet mogelijk zich goed te verantwoorden en kan het beleid minder goed worden uitgevoerd.

De informatie die door bewindspersonen wordt ontvangen en gecreëerd is essentiële overheidsinformatie. In het algemeen is bepaald dat deze informatie permanent te bewaren is. Deze informatie is nodig voor het uitvoeren van overheidstaken, het kunnen afleggen van verantwoording, het bieden van rechtszekerheid aan burgers en het mogelijk maken van onderzoek.

Voor wie is deze handreiking?

Tussen de departementen bestaan verschillende behoeften voor het voeren van een informatiehuishouding. Departementen bepalen zelf hoe ze overheidsinformatie duurzaam toegankelijk beheren, op maat van de eigen organisatie. De handreiking dient als hulpmiddel. Hij biedt een overzicht van de verplichtingen, uitgangspunten en aanbeveilingen bij het maken van de keuzes voor e-mails, socials en berichtenapps.

De handreiking is primair gericht op de ambtelijke organisaties binnen de departementen rondom de bewindspersonen. Aan hen de oproep om de informatie uit de handreiking te delen met relevante collega's. Denk aan politiek assistenten, informatieprofessionals en communicatieadviseurs.

Wat zijn de inhoud en insteek van deze handreiking?

De handreiking maakt inzichtelijk wat de wettelijke verplichtingen zijn bij het veiligstellen van informatie van bewindspersonen, hoe departementen hieraan kunnen voldoen en welke rechten en mogelijkheden er zijn om als departement regie te blijven voeren op informatie.

Deze handreiking richt zich op e-mail, chatberichten en sociale media, omdat bij deze communicatiekanalen acties van de bewindspersonen zelf nodig zijn en er (nog) geen automatische oplossingen zijn ontwikkeld voor het adequaat veiligstellen van de informatie. In veel gevallen is het van belang dat de bewindspersoon hier vooraf zelf acties uitvoert, om op een later moment werk te besparen of problemen te voorkomen.

1 Veiligstellen van informatie betekent niet dat alle zakelijke informatie meteen openbaar en inzichtelijk is voor iedereen. Veiligstellen is een puur technische handeling die zorgt dat informatie niet langer gewijzigd of verwijderd kan worden. De gebruikte techniek kan verschillen.
'Onder beheer brengen' betekent meer dan veiligstellen. Je stelt het dan niet alleen veilig, maar je plaats het ook in een bepaalde context en maakt het mogelijk om beheershandelingen uit te voeren (zoals vernietigen of overbrengen).

De wetgever maakt geen onderscheid tussen communicatiekanalen. **Dit betekent dat alle zakelijke e-mails, zakelijke informatie op sociale media en zakelijke chatberichten moeten worden beheerd.**

De handreiking is gebaseerd op geldend beleid en huidige richtlijnen. Waar beleid nog niet is geformuleerd, geven we advies in de vorm van aanbevelingen, werkwijzen of praktische tips.

De bewindspersoon is en blijft zelf eindverantwoordelijk voor de eigen informatiehuishouding. Het is raadzaam om in een vroeg stadium het gesprek aan te gaan met de bewindspersoon over informatiehuishouding en de werkwijze van het departement.

Naast deze handreiking is er ook een handreiking voor de bewindspersonen zelf. Die variant is beknopter en gaat in op de hoofdpunten van het goed inregelen van de eigen informatiehuishouding. De aanbevelingen voor de bewindspersonen in die variant staan in de Bijlagen (hoofdstuk 5, bladzijde 17).

Bijlagen: Overzicht van de aanbevelingen in de handreiking voor bewindspersonen

1.1 Wat is informatiehuishouding?

Informatiehuishouding is het geheel aan regels, structuren, processen en voorzieningen voor het gebruik en beheer van informatie. Denk aan het creëren, opslaan, ordenen, bewaren, ontsluiten, verstrekken en vernietigen van informatie.

Informatiehuishouding omvat zowel fysieke documenten en dossiers als digitale informatie, inclusief de informatie uit communicatiekanalen als e-mail, chatdiensten en sociale media. Digitale informatie kan variëren van Word-documenten, Excel-bestanden, PowerPoint-presentaties, e-mails, foto's, video's, illustraties en gescande brieven tot een gescand bierviltje met afspraken.

1.2 Waarom is een goede informatiehuishouding belangrijk?

Overheidsinformatie is niet alleen van en voor de overheid zelf, maar wordt ook gecreëerd en verzameld voor het algemeen belang. De samenleving heeft het recht en rechten om deze informatie in te zien. Een goede informatiehuishouding draagt bij aan inzicht in het handelen van de overheid, waardoor het parlement en de samenleving hun controlerende taak kunnen uitvoeren. Dit is essentieel voor het waarborgen van de kwaliteit van besluitvorming en bestuur en het vertrouwen in de overheid.

Ook voor de interne bedrijfsvoering is het belangrijk dat de informatiehuishouding op orde is. Alleen dan is informatie gemakkelijk en snel te vinden, door de juiste persoon, op het gewenste moment. Dit komt binnen de dagelijkse werkzaamheden de efficiëntie en de samenwerking ten goede. Daarnaast draagt een goede informatiehuishouding bij aan de bescherming van persoonsgegevens en andere vertrouwelijke informatie. Het zorgt ervoor dat persoonsgegevens en vertrouwelijke informatie veilig worden opgeslagen en zijn beschermd tegen misbruik.

Als de informatiehuishouding op orde is, is alle informatie op het juiste moment in een bepaald proces voor de juiste persoon in de juiste vorm beschikbaar[2]. Nu en in de toekomst.
Het grote belang van transparantie en een informatiehuishouding op orde werd pijnlijk duidelijk bij de Toeslagenaffaire en de tragische gevolgen ervan. Het rapport van de Parlementaire Ondervragingscommissie Kinderopvangtoeslag (POK) heeft geleid tot een kabinetsreactie waarin onder meer staat dat openheid vanuit de overheid naar de samenleving de standaard moet zijn. De kwestie heeft ervoor gezorgd dat het verbeteren van de informatiehuishouding bij de Rijksoverheid hoog op de agenda staat.

1.3 Welke wet- en regelgeving is (o.a.) van toepassing?

Volgens de inlichtingenplicht uit artikel 68 uit de Grondwet zijn bewindspersonen verplicht om de Eerste en Tweede Kamer in te lichten. Daarnaast is de volgende wet- en regelgeving van invloed op de informatiehuishouding van de overheid:

1. **De Archiefwet** zorgt ervoor dat overheden hun informatie op een goede, geordende en toegankelijke manier beheren. Zodat de informatie die daarvoor in aanmerking komt voor de eeuwigheid kan worden bewaard of tijdig wordt vernietigd.
2. **De AVG** (**Algemene Verordening Gegevensbescherming**) beschermt de privacy van individuen door regels te stellen aan het verzamelen, opslaan, verwerken en delen van persoonlijke gegevens en legt verantwoordelijkheden bij organisaties die persoonsgegevens verwerken.
3. **De Woo** (**Wet open overheid**) regelt het recht van de burger om informatie op te vragen van de overheid zodat het handelen van de overheid gecontroleerd kan worden. Informatie wordt in principe openbaar gemaakt op basis van de wet of op verzoek, tenzij er gegronde redenen zijn dit niet te doen. De Woo heeft als doel overheidsorganisaties transparanter te maken, zodat deze zichzelf beter kunnen verantwoorden naar de samenleving.
4. **BIO** (**Baseline Informatiebeveiliging Overheid**) geeft regels voor de beveiliging van de informatie(-systemen) in alle bestuurslagen en bestuursorganen van de overheid.

1.4 Over welke informatie gaat het?

Alle zakelijke informatie valt onder de Archiefwet en de Woo en moet worden beheerd, zodat de informatie toegankelijk is. Dit betekent dat alle zakelijke informatie in alle communicatiekanalen moet worden beheerd. Hieronder vallen **níet** privé-informatie en partijpolitieke informatie. Deze soorten informatie vallen niet onder de Archiefwet of de Wet open overheid. De bewindspersoon mag dus zelf beslissen wat hiermee wordt gedaan en mag het zelf verwijderen. Voor zakelijke informatie geldt dit niet.

In het volgende hoofdstuk staat welke soorten informatie de wet onderscheidt en wat dit betekent voor het veiligstellen van informatie van de bewindspersonen. Door het onderscheid tussen soorten informatie scherp te hebben, wordt het risico kleiner dat privé- of partijpolitieke informatie van bewindspersonen toch onder beheer worden gebracht en mogelijk openbaar worden gemaakt.

2 https://www.informatiehuishouding.nl/over-informatiehuishouding

Deze zaken goed regelen bij de start van de ambtstermijn zorgt voor een efficiënte informatiehuishouding. Anders hebben ambtenaren op de departementen veel uitzoekwerk achteraf en moet de bewindspersoon alsnog de controleslag op privé-informatie uitvoeren.

Een goed begin is hier letterlijk het halve werk.

1.5 Wat is zakelijk, privé en partijpolitiek?

Er wordt onderscheid gemaakt tussen drie soorten informatie[3]:

- **Zakelijke informatie:** Informatie die gerelateerd is aan de taakuitoefening van de betrokken personen en uitgewisseld wordt uit hoofde van hun functie. Dus: alle informatie die de bewindspersoon maakt, deelt of ontvangt bij de uitvoering van betreffende taken. Deze informatie valt onder de Archiefwet en de Wet open overheid (Woo) en moet **wel** worden beheerd.
- **Privé-informatie:** De definitie van privé-informatie is tweeledig:
  - Allereerst gaat het om *met wie* er wordt gecommuniceerd. Gaat het om een privépersoon, niet zijnde een werk- of bestuurlijk contact, en wordt er alleen over privézaken gecommuniceerd, dan is het bij uitstek privé-informatie.
  - Daarnaast gaat het om *de inhoud* van de communicatie. Is de informatie niet bestuurlijk maar puur privé van aard, dan is het ook privé-informatie. Ook als het gericht is aan een werk- of bestuurlijk contact. Denk aan felicitaties en condoleances.

  Deze informatie valt niet onder de Archiefwet en hoeft **niet** te worden bewaard.
- **Partijpolitieke informatie:** Berichten van bewindspersonen met partijgenoten over onderwerpen die hun partij aangaan[4]. Dit kan betrekking hebben op zowel interne partijaangelegenheden als inhoudelijke partijpolitieke standpunten. Deze informatie valt niet onder de Archiefwet of de Woo en hoeft **niet** te worden bewaard.

Algemeen advies
In alle gevallen is het essentieel voor een goede informatiehuishouding om vooraf te bepalen hoe zakelijke, privé- en partijpolitieke informatie worden gescheiden en het daarna structureel uit te voeren.

In de kern raakt dit advies de essentie van het huidige beleid. Dit geldt dan ook voor iedere communicatievorm en binnen ieder departement.

3 Kabinetsreactie op de adviesrapporten over chatberichtenarchivering en informatiebeheer, 6 april 2023.
4 In de kabinetsreactie wordt het volgende geschreven over politiek assistenten: 'Deze medewerkers worden niet als sleutelfunctie aangemerkt en mogen chatberichten op hun telefoon laten staan en zelf hun chatgeschiedenis desgewenst verwijderen (NB: Hiervoor is aanpassing van de Archiefwet nodig)'.

Voorbeelden van privé-informatie

- Conversaties over sociale en privéaangelegenheden naar en van familie en vrienden. Deze kunnen ook gericht zijn aan een zakelijk contact. Het gaat om de *inhoud* van het bericht, De afzender of ontvanger is een eerste indicatie dat het gaat om een privébericht maar dit is dus niet het énige criterium. Zie hiertoe het volgende voorbeeld.
- Conversaties over sociale en privéaangelegenheden naar/van (leden van) organisaties waarvan u niet lid bent uit hoofde van uw functie. Denk bijvoorbeeld aan een trainer van een sportclub.
- Berichten van of naar collega's of andere zakelijke contacten met persoonlijke mededelingen, zoals een bericht over een verloren tas, een traktatie, condoleances en felicitaties.

Voorbeelden van partijpolitieke informatie

- Conversaties over het partijprogramma of een partijcongres.
- Berichten tussen bewindspersonen van dezelfde partij over een in te nemen standpunt in een bestuurlijke kwestie, bezien vanuit het oogpunt van de politieke partij.

Let op: het uiteindelijke inhoudelijk uitgedragen standpunt van de eerste verantwoordelijke bewindspersoon uit hoofde van de functie geldt als bestuurlijk standpunt en is daarmee niet langer (enkel) partijpolitiek van aard, maar heeft zakelijke waarde en valt daarmee onder zakelijke informatie.

1.5.1 Openbaarheid en restricties aan openbaarheid van overheidsinformatie

Opvragen informatie door derden

Als er via een informatie- of Woo-verzoek zakelijke informatie wordt opgevraagd, wordt deze naast de wettelijke uitzonderingsgronden gelegd. Dit gebeurt om te voorkomen dat het openbaar maken van deze informatie schadelijke gevolgen heeft voor bijvoorbeeld de veiligheid van een (bewinds)persoon of het landsbelang. In deze gevallen wordt de informatie niet vrijgegeven of worden delen van de informatie in de geleverde documenten onleesbaar gemaakt (gelakt). Dit geldt ook voor bijzondere persoonsgegevens[5]. Maar het uitgangspunt van de Woo bij overheidsinformatie blijft wel 'openbaar, tenzij'.

Overbrenging en openbaarheidsbeperkingen

Informatie die permanent moet worden bewaard, wordt uiteindelijk overgebracht naar het Nationaal Archief. Op dat moment worden ook eventuele tijdelijke (tot 100 jaar) openbaarheidsbeperkingen vastgelegd. De zorgdrager/het departement bepaalt dit, na advies van het Nationaal Archief.

De gronden voor een openbaarheidsbeperking zijn:

1. **Eerbiediging van de persoonlijke levenssfeer:** Denk hierbij aan documenten over reputatie, gedrag, financiële situatie of afbeeldingen die inbreuk maken op de persoonlijke levenssfeer. Ook kunnen andere wetten van toepassing zijn zoals de Wet geneeskundige behandelovereenkomst, de Wet politiegegevens of de Wet op de inlichtingen- en veiligheidsdiensten.
2. **Het belang van de staat of zijn bondgenoten:** Denk aan informatie over (militaire) inlichtingen- en veiligheidsdiensten en de diplomatieke dienst. Hieronder valt bijvoorbeeld informatie over de opbouw, paraatheid en inzet van de krijgsmacht, de beveiliging van onderdelen van de overheid en het bedrijfsleven die van vitaal belang zijn voor het maatschappelijk leven en informatiebeveiliging.

5 Lees meer over bijzondere persoonsgegevens.

3. **Onevenredige bevoor- of benadeling:** Denk hierbij aan informatie over de betrekkingen van Nederland met andere staten, het economische/financiële belang van de staat, maar ook de bevoor- of benadeling van natuurlijke personen. De nadruk bij deze beperking licht op de term 'onevenredig'. Een heel praktisch voorbeeld waarop deze beperking van toepassing is zijn de ministerraadstukken.

Beperkt openbare archieven kunnen alleen worden ingezien onder bepaalde voorwaarden. Met de toekomstige ingang van de Nieuwe Archiefwet zitten de beperkingsgronden van deze wet en de Woo op één lijn.

Op grond van de AVG mogen bijzondere persoonsgegevens niet langer en op meer plekken worden bewaard dan nodig is voor het doel waarvoor ze zijn verwerkt. Zakelijke e-mails met bijzondere persoonsgegevens moeten daarom worden uitgezonderd van beheer als zeker is dat alle informatie (zolang als nodig) elders in de organisatie wordt bewaard.

2. Aantreden Bewindspersonen: Omgang met e-mails, chatberichten en sociale media

Hoe gaan we op de juiste manier om met informatie in e-mail, chatdiensten en sociale media, zodat deze zo nodig kan worden beheerd.

2.1 E-mail

Uitgangspunten voor het onder beheer brengen van e-mail van bewindspersonen:

- **Scheid privé-, partijpolitieke en zakelijke informatie.**
- **Maak gebruik van een zakelijk account en een privé-account** voor de daarbij horende communicatie.
- **Stuur geen zakelijke mails door naar het eigen privé-adres.**
- **Verwijder nooit zakelijke e-mails.** Partijpolitieke en privé-informatie mag wél worden verwijderd.
- **Informeer de bewindspersoon over de huidige werkwijze voor het onder beheer brengen van e-mail.**
- **Maak eventueel binnen het departement tijdelijke afspraken** over het veiligstellen van e-mail van de bewindspersonen in afwachting van een rijksbrede oplossing voor e-mailarchivering.

2.1.1 Huidige situatie en werkwijze

Er wordt momenteel gewerkt aan een rijksbrede oplossing voor automatische e-mail-archivering. In de tussentijd is de gangbare werkwijze binnen de Rijksoverheid dat e-mails automatisch worden veiliggesteld op de e-mailserver van het departement. Tussen deze e-mails kan ook privé- en partijpolitieke informatie zitten. Deze informatie hoeft niet te worden beheerd en moet worden aangemerkt als privé.

Voorsorterend op de toekomstige Rijksbrede oplossing is het volgende al wél toe te passen op het gebied van e-mail. Verplaats privé- en partijpolitieke informatie naar een mapje ‘Privé’. Deze optie komt uit de Gedragsregeling, die zegt dat een medewerker een map kan aanmaken met ‘Privé’ in de naam die de werkgever alleen in zeer uitzonderlijke gevallen mag inzien.

Let op: dat heeft op dit moment geen effect, maar is raadzaam voor toekomstige oplossingen en om ervoor te zorgen dat heeft bij het op termijn overbrengen naar het Nationaal Archief de privé-informatie en partijpolitieke informatie uitgezonderd zal worden.

Let op: Bij een e-mail die zowel privé- en/of partijpolitieke informatie als zakelijke informatie bevat, weegt het overheidsbelang zwaarder. Een dergelijke e-mail valt onder de Archiefwet en moet worden beheerd.

2.2 Chatberichten

Uitgangspunten voor de omgang met chatberichten voor bewindspersonen:

- **Scheid privé-, partijpolitieke en zakelijke communicatie.**
- **Verwijder zakelijke informatie niet.** Partijpolitieke en privé-informatie mag wél worden verwijderd.
- **Beperk het gebruik van chatberichten voor zakelijke communicatie zoveel mogelijk** tot algemene mededelingen, informele zaken of een hulpvraag.
- **Deel geen bijzondere persoonsgegevens** (zoals medische informatie) **of vertrouwelijke informatie** via chatdiensten.
- **Houd zakelijke informatie op zakelijke apparatuur**, zoals een zakelijke telefoon, laptops of tablet. Gebruik bijvoorbeeld twee telefoons, één zakelijk en één privé.
- **Maak een zakelijk cloud-account aan voor de bewindspersoon dat is gekoppeld aan de zakelijke telefoon.** Dit voorkomt dat zakelijke informatie alsnog in een privécloud komt te staan als back-up.
- **Lees de zakelijke chatberichten van de zakelijke telefoon van de bewindspersoon periodiek uit.** Overleg wat het meest logische moment is om dit te doen, bijvoorbeeld tijdens specifieke overleggen.
- **Maak binnen het departement afspraken over het onder beheer brengen van chatberichten, leg deze vast en informeer de bewindspersoon hierover.**
- **Controleer of de optie om de berichten automatisch te verwijderen is uitgezet in de chatapplicatie.**

2.2.1 Huidige situatie en werkwijze

Op basis van de kabinetsreactie van 6 april 2023 waarin de hoofdlijnen van het chat-archiveringsbeleid zijn vastgesteld, wordt beleid uitgeschreven en een duurzame, geautomatiseerde oplossing voor chatarchivering ontwikkeld. In de tussentijd gebeurt het onder beheer brengen handmatig. Het is van belang dat dit op de juiste manier gebeurt. Om informatieverlies te voorkomen stellen departementen chatberichten periodiek veilig.

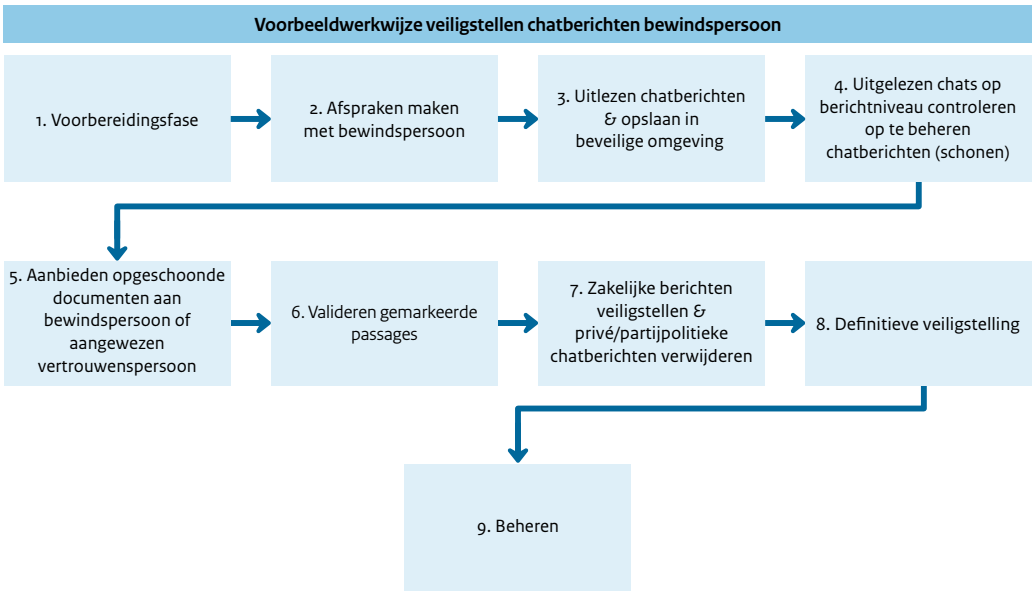
In de praktijk zal dit betekenen dat een medewerker van het departement periodiek de zakelijke chatberichten op de telefoon van de bewindspersoon zal (laten) uitlezen[6]. Uitlezen van de telefoon betekent niet automatisch dat alle berichten onder beheer komen. Er zal (door een medewerker) per contactpersoon, conversatie en soms zelfs per bericht gekeken moeten worden welke informatie wel en niet zakelijk is en dus onder beheer moet worden gebracht. Uiteindelijk wordt dit ter akkoord aangeboden aan de bewindspersoon of een aangewezen vertrouwenspersoon.

Hoe beter de zakelijke, privé- en partijpolitieke informatie vooraf wordt gescheiden, des te minder hoeven de chatberichten achteraf doorgelopen te worden. Daarom is het belangrijk dat bewindspersonen een zakelijke telefoon gebruiken voor hun communicatie als bewindspersoon en een privé-telefoon voor privé- en partijpolitieke communicatie. Bijkomend voordeel: de wellicht oncomfortabele gedachte dat de telefoon afgestaan moet worden, kan zo worden geminimaliseerd.

6 Als een departement de dienst afneemt bij Doc-Direkt doet een van hun medewerkers dit.

2.2.2 Toekomstige werkwijze

In afwachting van een rijksbrede technische oplossing voor het onder beheer brengen van chatberichten is er een aantal algemene processtappen die departementen als ze willen kunnen gebruiken als advies voor hun eigen werkwijze[7]. Na de figuur worden de verschillende stappen toegelicht.



1. Voorbereidingsfase

In de voorbereidingsfase stelt het departement een document op met de procesinrichting en werkafspraken. Hierin worden de samenwerking, uitvoering, verschillende rollen en taakverdelingen vastgelegd.

Het departement bespreekt de werkwijze met de bewindspersonen. Tijdens dit gesprek krijgt de bewindspersoon informatie en wordt gecommuniceerd wat de afspraken zijn voor het uitlezen van de telefoon. Er wordt geïnventariseerd welk type telefoon en welke apps de bewindspersoon gebruikt en in welke periode deze onder beheer moet worden gebracht (ambtsperiode).

2. Afspraken maken met bewindspersoon

Een informatieprofessional maakt (via het secretariaat) concrete afspraken met de bewindspersoon over het uitlezen van de telefoon en het markeren van chatberichten die privé of partijpolitiek zijn. De bewindspersoon markeert chatberichten die privé- of partijpolitiek zijn en niet in de beheerde en beveiligde omgeving moeten worden opgenomen. Alle berichten worden door de informatieprofessional in de volgende stap gecontroleerd om een vierogen principe te hanteren.

3. Uitlezen chatberichten en opslaan in beveiligde omgeving

Er wordt een afspraak gemaakt tussen de bewindspersoon en een informatieprofessional van het departement om de chatberichten te exporteren naar een beheerde en beveiligde omgeving: het uitlezen van de telefoon. Het is raadzaam dit voor een aantal maanden vooruit te plannen tijdens momenten waarop de bewindspersoon de telefoon niet nodig heeft. De uitgelezen chatberichten worden opgeslagen in een beveiligde omgeving.

7 Gebaseerd op Procesorganisatie Berichtenapps Archivering Doc-Direkt.

4. **Uitgelezen chats controleren op berichtniveau (schonen)**
   De informatieprofessional schoont de zakelijke chatberichten op. Bijzondere persoonsgegevens, privégesprekken en partijpolitieke gesprekken worden verwijderd.

5. **Aanbieden opgeschoonde documenten aan bewindspersoon of aangewezen vertrouwenspersoon**
   De informatieprofessional brengt de bewindspersoon op de hoogte dat de opgeschoonde berichten klaar zijn voor validatie en autoriseert de bewindspersoon voor de laatste controle.

6. **Valideren gemarkeerde berichten**
   De bewindspersoon beoordeelt de gemarkeerde berichten en geeft aan of deze inderdaad moeten worden verwijderd. Als er gemarkeerde berichten zijn die niet moeten worden verwijderd, gaat de bewindspersoon hierover het gesprek aan met de informatieprofessional.

7. **Zakelijke berichten onder beheer brengen en privé- en partijpolitieke chatberichten verwijderen**

8. **Definitief onder beheer brengen**
   Na goedkeuring wordt de geschoonde chatinformatie definitief veiliggesteld voor archivering.

9. **Beheren**
   De definitief onder beheer gebrachte informatie wordt opgeslagen in een omgeving waar deze wordt beheerd en op termijn kan worden overbracht.

2.3 Sociale media

Rijksbeleid en bijbehorende richtlijnen over het onder beheer brengen van overheidsinformatie op sociale media is op het moment van publiceren van deze handreiking nog in ontwikkeling. In afwachting hiervan een aantal handvatten en adviezen om het onder beheer brengen van overheidsinformatie op sociale media achteraf zo eenvoudig mogelijk te maken. Want ook hier geldt: vooraf goed inregelen scheelt veel tijd en monnikenwerk achteraf.

Praktische aanbevelingen voor de omgang met van informatie van bewindspersonen op sociale media:

- **Maak gebruik van corporate accounts voor het delen van overheidsinformatie op sociale media.**
- Adviseer de bewindspersoon **alleen overheidsinformatie via corporate accounts** in naam van uw departement te delen.
- **Verwijder overheidsinformatie op sociale media van voorgaande bewindspersonen pas nadat de informatie is veiliggesteld binnen de beheerde informatiesystemen van de organisatie en beschikbaar is voor eventuele openbaarmaking.** Het is mogelijk dat burgers inhoudelijke vragen stellen over de communicatie uitingen van de vorige bewindspersoon. Voorkomen moet worden dat door het verwijderen van deze informatie geen mogelijkheid meer deze informatie te verstrekken om deze vragen te beantwoorden.
- **Benoem op het sociale medium dat alle informatie onder beheer wordt gebracht**, zodat burgers weten dat deze informatie wordt bewaard.
- **Informeer de bewindspersoon samen met de communicatie-afdeling.** Dan kan gezamenlijk besproken worden welke werkafspraken bestaan of gemaakt kunnen worden over het gebruik, veiligstellen en beheer van sociale media.
- **Het is raadzaam om hybride accounts te laten beheren door medewerkers binnen het departement**, zodat de overheidsinformatie op deze accounts eenvoudig onder beheer kan worden gebracht.

Uitleg bij voorgaande aanbevelingen

Zakelijke informatie die bewindspersonen plaatsen en ontvangen op sociale media is overheidsinformatie. Dit geldt voor de posts, het profiel en de reacties[8]. Daarmee valt deze informatie onder de Archiefwet en de Woo.

We onderscheiden drie verschillende soorten accounts:

1. **Corporate accounts:** dit zijn zakelijke accounts in naam van de overheidsorganisatie, bijvoorbeeld @minBZK en @minpres. Deze accounts worden door de organisatie aangemaakt en beheerd, en zijn bedoeld om informatie te delen over onderwerpen die betrekking hebben op die overheidsinstantie.
2. **Hybride accounts:** dit zijn accounts die de naam van een organisatie of bewindspersoon dragen maar vaak wel beheerd worden in samenwerking met de politieke of ambtelijke ondersteuning.
3. **Persoonlijke accounts:** dit zijn accounts die de naam van de bewindspersoon dragen en die volledig worden beheerd door de bewindspersoon zelf.

8 Hiervoor is in de Whitepaper SMA de oproep gedaan om een antwoord te formuleren op de vraag hoe in de praktijk om te gaan met deze vorm van overheidsinformatie.

Alle informatie die wordt gedeeld via een **corporate account** moet per definitie worden veiliggesteld en worden beheerd.

Deze duidelijkheid ontbreekt bij **hybride en/of persoonlijke accounts**. Deze kunnen zowel overheids- als privé- en partijpolitieke informatie bevatten. Dit laatste maakt het onder beheer brengen van de overheidsinformatie ingewikkelder.

Het standaard advies is dat persoonlijke accounts niet worden gebruikt voor overheidsinformatie over de publieke taak. Op het moment dat dit wel gebeurt, moet deze informatie worden beheerd. Het onder beheer brengen van overheidsinformatie op persoonlijke accounts is ingewikkeld en tijdsintensief.

Daarnaast is het raadzaam om hybride accounts te laten beheren door medewerkers binnen het departement, zodat de overheidsinformatie op deze accounts eenvoudig onder beheer kan worden gebracht. Tijdens het onder beheer brengen van overheidsinformatie op deze accounts moeten medewerkers van het departement de privé- en partijpolitieke informatie indien mogelijk uitfilteren.

3. Aftreden bewindspersoon

Als een bewindspersoon aftreedt, is het van belang dat alle zakelijk informatie onder beheer wordt gebracht en informatieverlies wordt voorkomen. Als de aanbevelingen uit deze handreiking tijdens de ambtstermijn zijn opgevolgd en nageleefd, ligt bij het aftreden de nadruk op het onder beheer brengen van alle informatie die nog niet onder beheer was gebracht en het inleveren van de zakelijke apparaten. Dan zijn immers dezelfde wetten, beleidsregels en richtlijnen van toepassing als bij het aantreden. Daarnaast zijn er nog enkele andere aandachtspunten van belang bij het vertrek van bewindspersonen.

In dit hoofdstuk wordt een aantal zaken op een rij gezet die kunnen dienen als checklist voor de ambtelijke organisaties bij het onder beheer brengen van zakelijke informatie van bewindspersonen.

Algemeen

- Communiceer naar de bewindspersoon dat alle privé- en partijpolitieke informatie moet zijn gescheiden, gemarkeerd of verwijderd vóór vertrek, zodat deze onder beheer kan worden gebracht. Dit geldt voor e-mails, chatberichten en overheids-informatie op sociale media.
- Het is onwenselijk om bewindspersonen en ambtenaren toe te staan zakelijke overheidsinformatie, ook in chatberichten en e-mails, mee te nemen. Informatie die puur privé of partijpolitiek van aard is mag wel worden meegenomen.
- Communiceer naar de bewindspersoon dat de zakelijke ICT-middelen voor het aftreden moeten worden ingeleverd.
- Het meenemen van mobiele contacten moet gebaseerd zijn op een functionele noodzaak. Anders wordt ook afgeraden om deze contacten mee te nemen.

Het niet voldoen aan de bovenste vier punten brengt reële risico's met zich mee op het gebied van informatieverlies, datalekken, veiligheidsrisico's en privacy schending.

E-mail

- Adviseer geen zakelijke e-mails door te sturen naar het eigen privé-mailadres.

Chatberichten

- Laat de mobiele telefoon van de bewindspersoon uitlezen voor vertrek. De telefoon kan na het uitlezen van de chatberichten meteen worden ingeleverd.
- In het geval dat nog niet is gebeurd: maak een zakelijke cloud-account aan voor de bewindspersoon, gekoppeld aan het zakelijke apparaat om te voorkomen dat er een back-up van de chatberichten wordt meegenomen naar een privé-account.
- Controleer of de optie om de berichten automatisch te verwijderen is uitgezet in de chatapplicatie.

Sociale media

- Communiceer naar de bewindspersoon om tot nader order geen zakelijke informatie van het publieke domein te verwijderen.

4. Bijlage: Overzicht van de aanbevelingen opgenomen in de handreiking voor bewindspersonen

Dit overzicht kan worden gebruikt als praktische praatplaat of checklist bij het aantreden van nieuwe bewindspersonen.

Algemeen:

- Scheid privé-, partijpolitieke en zakelijke informatie. Dit kunt u op de volgende manieren aanpakken:
  - Gebruik een zakelijk account en een privé-account voor de daarbij horende communicatie.
  - Houd zakelijke informatie op zakelijke apparatuur. Het gaat hier om telefoons, laptops en tablets.
- Verwijder in geen geval zakelijke informatie. Privé- en Partijpolitieke informatie mogen desgewenst wél worden verwijderd.
- Weet wat u moet doen voor het onder beheer brengen van informatie. Als bewindspersoon wordt u geïnformeerd door de betreffende medewerkers binnen uw departement.

E-mail:

- Gebruik geen privé-mailadres voor zakelijke doeleinden.
- Stuur geen zakelijke mails door naar het eigen privé-mailadres.
- Deel geen staatsgeheime informatie via e-mail.
- Uw zakelijke e-mailaccount wordt automatisch gearchiveerd. Hiervoor zijn geen acties nodig.

Chat:

- Beperk het gebruik van berichtenapps voor zakelijke communicatie zoveel mogelijk tot algemene mededelingen, informele zaken, of een hulpvraag. Gebruik ze niet voor persoonsgegevens en/of voor formele zaken zoals bestuurlijke aangelegenheden.
- Deel geen bijzondere persoonsgegevens (zoals medische informatie) of vertrouwelijke informatie via chatapplicaties.
- Controleer of de optie om berichten automatisch te verwijderen is uitgezet in de chatapplicatie.
- De zakelijke chatberichten op uw zakelijke telefoon worden periodiek uitgelezen. In overleg met uw secretariaat wordt hiervoor een geschikt moment gekozen.

Sociale media:

- Maak gebruik van corporate accounts voor het delen van overheidsinformatie op sociale media. U wordt door uw adviseurs geïnformeerd over welke overige werkafspraken bestaan of gemaakt kunnen worden over het gebruik, veiligstellen en beheer van sociale media.

Versiebeheer

25-01-2024	0.5 (Projectgroep & CIO-Rijk)
31-01-2024	0.6 (Projectgroep & CIO-Rijk)
08-02-2024	0.8 (Klankbordgroep bestaande uit I-professionals departementen)
21-02-2024	0.9 (Afvaardiging HBSG, klankbordgroep, CIO-rijk & projectgroep)
04-03-2024	0.91 (Strategisch Beraad)
13-03-2024	0.99 (Afvaardiging HBSG, CIO-Rijk, Nationaal Archief, Jurist OCW)
	0.99 (Nationaal Archief op juiste terminologie)
25-03-2024	1.0 (verwerking annotaties HBSG)

Projectgroep:
- Ministerie van Defensie
- Ministerie van Financiën
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Nationaal Archief
- Doc-Direkt
- RDDI
- CIO-Rijk

Klankbordgroep:
- Ministerie van Algemene Zaken
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Ministerie van Buitenlandse Zaken
- Ministerie van Economische Zaken en Klimaat
- Ministerie van Infrastructuur en Waterstaat
- Ministerie van Justitie en Veiligheid

Afvaardiging HBSG:
- Ministerie van Economische Zaken en Klimaat
- Ministerie van Financiën
- Ministerie van Justitie en Veiligheid
- Ministerie van Landbouw, Natuur en Voedselkwaliteit
- Ministerie van Onderwijs, Cultuur en Wetenschap
- Ministerie van Sociale Zaken en Werkgelegenheid
- Ministerie van Volksgezondheid, Welzijn en Sport

Colofon

Programma	RDDI
Projectnaam	Handreiking IHH Kabinetswissel
Versienummer	1.0

Rijksprogramma Duurzame Digitale Informatiehuishouding (RDDI)

Rijnstraat 50 | Den Haag
Postbus 16375 | 2500 BJ Den Haag