Handreiking voor **bewindspersonen**

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

Inhoudsopgave

1. Inleiding

Deze handreiking geeft inzicht in wat u kunt doen om te voldoen aan de wet- en regelgeving voor de omgang met uw e-mail, chatberichten en sociale media. Het is belangrijk om hier aan de start van uw ambtstermijn bij stil te staan. Zo is de veiligstelling van uw informatie tijdens uw ambtstermijn goed geregeld en wordt informatieverlies bij aftreden voorkomen.

Als bewindspersoon draagt u persoonlijke verantwoordelijkheid voor uw handelen en daarmee ook voor de informatie die daarbij hoort[1]. Deze verantwoordelijkheid vloeit voort uit onder meer de Grondwet en de Archiefwet.

Op de juiste manier omgaan met informatie zorgt voor transparantie, verantwoording en efficiëntie. Een goede informatiehuishouding helpt de overheid gegevens beter op te slaan, te beheren en te delen en is daarmee een belangrijke component voor het reconstrueren van (totstandkoming van) handelen van de overheid. De huidige wetgeving vraagt hier ook om. Een belangrijke stap daarin is het veiligstellen en het onder beheer brengen van[2] van zakelijke informatie.

Door hiervoor meteen bij uw aantreden maatregelen te treffen, wordt het risico op verlies van informatie die hoort bij het uitvoeren van uw functie geminimaliseerd.

De wetgever maakt geen onderscheid tussen communicatiekanalen. **Dit betekent dat ook alle zakelijke informatie in e-mails, op sociale media en in chatberichten moet worden beheerd**, zodat deze kan worden veiliggesteld en uiteindelijk gearchiveerd.

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.

Toeslagenaffaire
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.

Deze handreiking geeft advies in de vorm van aanbevelingen of praktische tips voor het onder beheer brengen van e-mail, chatberichten en sociale media. Bij deze communicatiekanalen zijn acties nodig van u als bewindspersoon persoonlijk en er zijn (nog) geen of beperkte automatische oplossingen ontwikkeld voor het adequaat onder beheer brengen van deze informatie.

In het volgende hoofdstuk krijgt u concrete aanbevelingen. Daarna vindt u verdiepende uitleg over de verplichtingen waarop de aanbevelingen zijn gebaseerd en de verschillende soorten informatie die de wet onderscheidt. In de Bijlagen kunt u verdere achtergrondinformatie lezen over informatiehuishouding en de onderliggende wetgeving.

1 Als bewindspersoon bent u eindverantwoordelijk voor het juist omgaan met alle informatie van uw departement. Deze handreiking richt zich alleen op uw omgang met uw eigen e-mail, chatberichten en socialemediaberichten.
2 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).

2. Aanbevelingen bij het onder beheer brengen van e-mail, chatberichten en sociale media

Om e-mail, chatberichten en sociale media zo efficiënt mogelijk veilig te stellen, hebben we een aantal aanbevelingen op een rij gezet. Met deze aanbevelingen heeft u als bewindspersoon, maar ook de ambtelijke organisatie, achteraf zo min mogelijk werk bij het onder beheer brengen.

Algemeen:

- Scheid privé-, partijpolitieke en zakelijke informatie:
  - Gebruik een zakelijk account en een privé-account voor de daarbij horende informatie.
  - Houd zakelijke informatie op zakelijke apparatuur, zoals een zakelijke telefoon, laptop of tablet.
- Verwijder in geen geval zakelijke informatie. Privé- en partijpolitieke informatie mag 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 e-mails door naar uw privé-mailadres.
- Deel geen staatsgeheime informatie via e-mail.
- Uw zakelijk e-mailaccount wordt automatisch gearchiveerd. Hiervoor zijn geen acties nodig.

Chatberichten:

- Beperk het gebruik van berichtenapps voor zakelijke communicatie zoveel mogelijk tot algemene mededelingen en informele zaken, of een hulpvraag. Gebruik geen chatapplicaties voor formele zaken zoals bestuurlijke aangelegenheden en persoonsgegevens.
- 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.

3. Verdiepende uitleg: wat is zakelijke, privé- en partijpolitieke informatie?

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 u als bewindspersoon maakt, deelt of ontvangt bij de uitvoering van uw taak. 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 uw partij aangaan. Hieronder vallen zowel interne partijaangelegenheden als inhoudelijke partijpolitieke standpunten. Deze informatie valt niet onder de Archiefwet hoeft niet te worden beheerd.

Algemeen advies

In alle gevallen is het essentieel voor een goede informatiehuishouding om vooraf te bepalen hoe zakelijke, privé- en partijpolitieke informatie wordt 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.

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.

3 Kabinetsreactie op de adviesrapporten over chatberichtenarchivering en informatiebeheer, 6 april 2023.

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.

3.1 Opvragen informatie door derden

Als er via een informatie- of Woo-verzoek zakelijke informatie wordt opgevraagd, wordt deze eerst getoetst aan de wettelijke uitzonderingsgronden voor openbaarmaking. 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). Maar het uitgangspunt van de wetgeving bij overheidsinformatie blijft: ‘openbaar, tenzij’.

4. Bijlage 1: Achtergrondinformatie handreiking

4.1 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 en illustraties , gescande en op de computer opgemaakte brieven en zelfs tot een gescand bierviltje met afspraken.

4.2 Waarom is een goede informatiehuishouding belangrijk?

Overheidsinformatie is niet alleen van en voor de overheid, 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 het inzicht in het handelen van de overheid, waardoor het parlement haar controlerende taak kan uitvoeren. Dit is essentieel voor het waarborgen van de kwaliteit van besluitvorming en bestuur en draagt bij aan het vertrouwen in de overheid.

Daarnaast draagt een goede informatiehuishouding bij aan de bescherming van persoonsgegevens en andere vertrouwelijke informatie: persoonsgegevens en vertrouwelijke informatie worden veilig opgeslagen en zijn beschermd tegen misbruik.

Met een informatiehuishouding op orde is alle informatie op het juiste moment in een bepaald proces voor de juiste persoon in de juiste vorm beschikbaar[4]. Nu en in de toekomst.

Het uitgangspunt voor de informatiehuishouding van de overheid is transparantie en verantwoording naar de samenleving: burgers en bedrijven, maar ook journalisten, ambtenaren en andere politici.

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

4.3 Wetgeving

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.

Colofon

Programma	RDDI
Projectnaam	Handreiking IHH Kabinetswissel
Versienummer	0.99
Projectleider	Jeffrey Mangal
Projectadviseur	André van Arkel
Projectsecretaris	Jan Gesink

Rijksprogramma Duurzame Digitale Informatiehuishouding (RDDI)

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