Handreiking
Bewaren van e-mail Rijksoverheid

Rijksprogramma
Duurzaam
Digitale
Informatiehuishouding

Inhoudsopgave

Inleiding

In de digitale wereld is de hoeveelheid digitale overheidsinformatie extreem gegroeid. E-mail is inmiddels de voornaamste vorm van communicatie binnen het Rijk. Ter illustratie: Het aantal verzonden en ontvangen e-mails binnen het Rijk bedraagt naar schatting minstens een miljard per jaar. Er is een grote businesscase voor het verbeteren van de digitale informatiehuishouding binnen het Rijk.

De grote hoeveelheden e-mail die de gemiddelde rijksmedewerker verstuurt en ontvangt maakt het bijzonder complex en tijdrovend om de bestaande procedures te volgen, met als risico dat niet voldaan wordt aan de vereisten van de Archiefwet, de WOB en de AVG. De procedures zijn veelal nog ontworpen in het pre-digitale tijdperk.

De huidige situatie is enerzijds volkomen onvergelijkbaar met het pre-digitale tijdperk: er is veel meer informatie, er is veel meer technische complexiteit en er spelen vaker verschillende belangen tegelijkertijd, zoals publieke verantwoording en de beveiliging van systemen die 'anytime, anyplace' gebruikt worden. Anderzijds is de 'raison d'être' van het informatiebeheer onveranderd: de overheid moet haar eigen handelen kunnen reconstrueren.

Het informatiebeheer van de overheid moet zich op deze situatie instellen, zowel in praktijk als in regelgeving. Dit vraagt nadrukkelijk om een herziening van de werkwijze; door politiek en burgers die meer transparantie vragen en door de ontwikkeling van ICT die het informatiebeheer met nieuwe opgaven confronteert.

Het programma Rijk aan Informatie (RaI) heeft, in samenwerking met BZK/CIO Rijk en OCW, een nieuwe werkwijze ontwikkeld voor het bewaren van e-mail. Deze werkwijze maakt het mogelijk om wel te voldoen aan de vereisten van de Archiefwet, de WOB en de AVG op een manier die van individuele medewerkers minder vergt dan bestaande werkwijzen. Deze nieuwe werkwijze gaat uit van het zo min mogelijk belasten van de medewerker, gecombineerd met het slim en veilig terug kunnen vinden van informatie.

Deze handreiking is rijksbreed gereviewed. De werkwijze is tot stand gekomen na het opstellen van een whitepaper, het uitvoeren van pilots bij VWS en JenV, het uitvoeren van een Privacy Impact Analysis (PIA) en het uitvoeren van de volgende onderzoeken door het Nationaal Archief:

- Openbaarheid
- Duurzame toegankelijkheid
- Selectie van sleutelfunctionarissen
- Toepassing en Gebruiksgemak

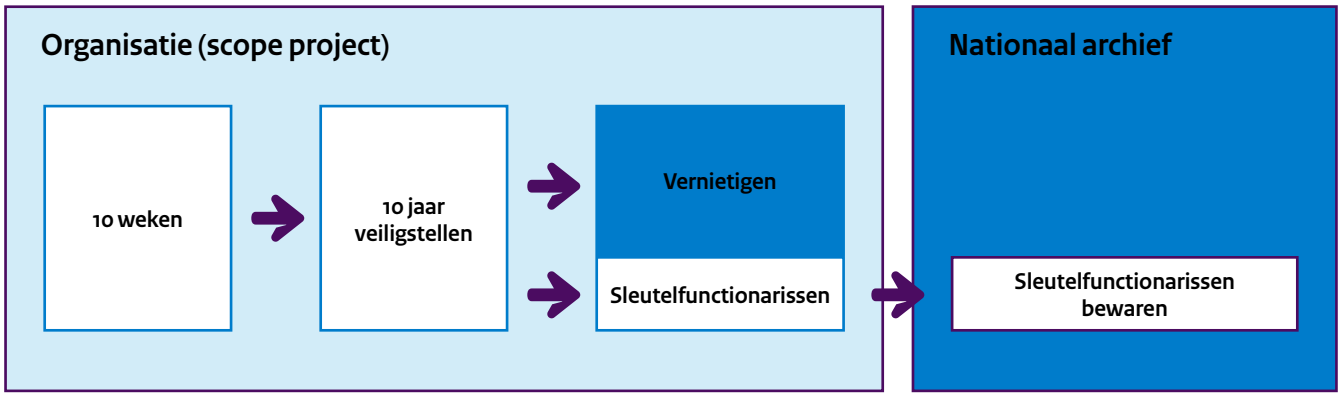
De handreiking is bedoeld voor organisaties van de Rijksoverheid.

1 Doelen

De nieuwe werkwijze beoogt het realiseren van een tweetal doelen.

- Het veiligstellen van de inhoud van de e-mailboxen van de Rijksoverheid, zolang de desbetreffende informatie beschikbaar moet zijn voor het behandelen van WOB-verzoeken, parlementaire enquêtes, etc.
- Het blijvend bewaren van de veiliggestelde e-mails die met het oog op toekomstig (historisch) onderzoek van waarde worden geacht. Blijvende bewaring houdt in dat informatie op termijn over wordt gebracht naar het Nationaal Archief, waar de betreffende e-mail door het publiek mag worden ingezien voor zover daar op grond van de Archiefwet geen beperkingen aan zijn gesteld.

2 Werkwijze op hoofdlijnen



- E-mail verzonden of ontvangen door medewerkers van de Rijksoverheid wordt tien weken na verzending of ontvangst automatisch veiliggesteld.
- Medewerkers worden in de eerste tien weken na verzending of ontvangst van e-mail in staat gesteld om niet relevante e-mails (waaronder privé e-mail, p-vertrouwelijke zaken of e-mail niet uit hoofde van functie verstuurd of ontvangen) uit te zonderen van automatisch veiligstellen.
- Alle e-mails worden tien jaar opgeslagen, waarna deze worden vernietigd.
- Hierop is een aantal uitzonderingen:
  - e-mail van aan te wijzen sleutelfunctionarissen wordt permanent bewaard;
  - e-mail van niet-sleutelfunctionarissen kan in bepaalde gevallen uitgezonderd worden van vernietiging en permanent bewaard worden;
  - e-mail met bijzondere persoonsgegevens kan waar nodig op verzoek worden vernietigd;
  - e-mail met een bij wet gestelde vernietigingstermijn korter dan tien jaar wordt na verstrijken van deze termijn vernietigd.
- Conform de termijn daarvoor gesteld in de Archiefwet wordt e-mail van sleutel-functionarissen en overige e-mail die als blijvend te bewaren is aangemerkt naar het Nationaal Archief overgebracht. Bij overbrenging kunnen organisaties openbaarheids-beperkingen aanbrengen.

3 Toelichting werkwijze

Bij het automatisch veiligstellen gaat het om de ontvangen en verzonden e-mailberichten, inclusief berichten in eventuele submappen. Berichten in de map 'verwijderde items' en berichten die zijn gemarkeerd als niet relevant worden niet veiliggesteld. Het veiligstellen heeft betrekking op zowel persoonsgebonden als functionele mailboxen ('dienstpostbussen').

Na tien weken zijn e-mails veiliggesteld en toegankelijk in geval van informatieverzoeken. Organisaties zijn in eerste instantie slechts gehouden om toegang te verstrekken indien dergelijke informatieverzoeken aan de orde zijn. Het hoeft dus geen 'werkarchief' te zijn waar medewerkers dagelijks e-mail voor de eigen bedrijfsvoering in kunnen terugvinden. Voor zover organisaties daar wel in gaan voorzien is het van belang dat e-mail dat na tien weken is veiliggesteld, niet door medewerkers zelf verwijderd kan worden. De veiliggestelde e-mail wordt, behoudens genoemde uitzonderingen, na tien jaar vernietigd.

Deze handreiking raakt niet aan bestaande primaire processen waarbij het kan voorkomen dat e-mail aan een dossier of zaak wordt toegevoegd.

4 Scope en vaststelling

De werkwijze is toe te passen door organisaties van de Rijksoverheid als aanvulling op, of alternatief voor, de huidig gangbare methode van veiligstellen van e-mail. Het moet daarbij mogelijk zijn om, waar nodig, bepaalde (uitvoerende) werkprocessen buiten scope te houden. Denk daarbij aan processen waarin bijzondere persoonsgegevens worden gedeeld of die te maken hebben met wettelijke vernietigingstermijnen, vastgelegd in sectorspecifieke wetgeving. Deze gegevens kennen absolute vernietigingstermijnen die bijvoorbeeld samenhangen met het moment van rechtelijke uitspraak of overlijden van een persoon. Dit zijn uitzonderingen op de vernietigingstermijn van tien jaar.

De werkwijze kan niet met terugwerkende kracht worden ingevoerd.

5 Wettelijke verplichtingen

En zijn een aantal wettelijke verplichtingen die op de Minister rusten bij het veiligstellen van e-mails. Hierbij moet in hoofdzaak aan de volgende verplichtingen worden gedacht:

- Op grond van de artikelen 3 en 8 van de Wet openbaarheid van bestuur is de Minister verplicht om desgevraagd, respectievelijke uit eigen beweging, informatie over bestuurlijke aangelegenheden die is neergelegd in documenten, openbaar te maken, behoudens de in die wet genoemde uitzonderingen en beperkingen. E-mails vallen onder de definitie van documenten;
- Op grond van artikel 68 van de Grondwet is de Minister verplicht om de Tweede en Eerste Kamer afzonderlijk en in verenigde vergadering mondeling of schriftelijk de door een of meer leden verlangende inlichtingen te geven, behoudens de daarbij genoemde uitzondering;
- Op grond van artikel 3 van de Archiefwet is de Minister verplicht om de onder hem berustende archiefbescheiden in goede, geordende en toegankelijke staat te brengen en te bewaren, alsmede zorg te dragen voor de vernietiging van de daarvoor in aanmerking komende archiefbescheiden. E-mails vallen onder de definitie archiefbescheiden.

6 Privacy & AVG

6.1 Persoonsgegevens

Met het opslaan van de e-mails worden ook persoonsgegevens verzameld. Het ligt in de aard van e-mail dat de inhoud ook bijzondere persoonsgegevens kan bevatten, conform artikel 9 van de AVG. Op grond van artikel 5, tweede lid, en de artikelen in hoofdstuk III en IV van de AVG is de Minister verplicht om inzichtelijk te hebben welke persoonsgegevens hij verwerkt en in staat om aan te kunnen tonen dat de verwerkingen daarvan voldoen aan de bepalingen van de AVG.

6.2 Rechtmatigheid

De verwerkingen dienen noodzakelijk te zijn voor het naleven van een wettelijke verplichting, de taak van algemeen belang, of de uitoefening van openbaar gezag. Dit betekent dat er niet meer moet worden veiliggesteld dan daarvoor nodig is. In termen van rechtmatigheid en behoorlijkheid (art. 5, eerste lid, onder a, AVG) wordt dit onder andere geborgd doordat de medewerker gedurende tien weken in de gelegenheid wordt gesteld om zelf de e-mail-berichten te verwijderen die naar zijn oordeel voor de naleving van de wettelijke plicht of de taak van algemeen belang niet veiliggesteld hoeven te worden.

6.3 Rechtmatigheid verdere verwerking

Waar het gaat om het veiligstellen van de e-mailberichten, is van belang dat in de preambule van de AVG wordt opgemerkt dat de bepaling waarvan gebruik wordt gemaakt als rechtsgrond voor de oorspronkelijke verwerking, ook kan dienen als rechtsgrond voor verdere verwerking (overweging 50 AVG), dat wil zeggen veiligstelling. Verder kan worden gewezen op de verplichting van artikel 3 Archiefwet.

6.4 Doelbinding

Voor de doelbinding is verder relevant dat de mogelijke gevolgen voor de betrokkenen van het veiligstellen van de berichten en het op- of doorzoeken daarvan, niet onevenredig en nadelig zijn (art 6, vierde, lid, onder d, AVG). En daarvoor is van belang dat, in het geval van een informatieverzoek, bij de besluitvorming daarover hoe dan ook de privacybelangen van deze medewerker worden afgewogen tegen het belang bij openbaarmaking. Oftewel, als e-mailberichten gedurende tien jaar worden veiliggesteld, en in geval van sleutel-functionarissen permanent worden bewaard, is daarmee niet gezegd dat daarmee de persoonlijke levenssfeer wordt aangetast, en als dat zou gebeuren, dan alleen na een belangenafweging.

6.5 Kenbaarheidsprincipe

Bij het invoeren van de werkwijze dient een helder kenbaarheidsprincipe te zijn toegepast. Organisaties die de werkwijze invoeren dienen een aparte privacyverklaring op te stellen waarin duidelijk is verwoord hoe met persoonsgegevens wordt omgegaan en hoe de betrokkene gebruik kan maken van zijn rechten. Deze privacyverklaring moet algemeen toegankelijk zijn. Het verdient de voorkeur om, op die plekken waar e-mailadressen van rijksmedewerkers bekend worden gemaakt, of in de e-mail zelf, aan te geven dat de zgn. 'Handreiking Bewaren van e-mail Rijksoverheid' van toepassing is.

Tevens dient de medewerker geïnformeerd over de mogelijke privacyrisico's en aangeven welke maatregelen hij kan nemen (bv. geen privémails vanuit werkaccounts versturen, geen bijzondere persoonsgegevens in e-mails). Deze awareness campagnes moeten een continu karakter hebben.

6.6 Recht op inzage

Bij het inrichten en vormgeven van de nieuwe werkwijze moet rekening worden gehouden met het kunnen voldoen aan verzoeken op grond van de verschillende rechten van betrokkenen (privacy by design).

Een betrokkene heeft het recht om inzage te verkrijgen, tenzij dit verzoek zodanig ongericht is dat dit in redelijkheid niet kan worden ingewilligd (art. 45, tweede lid, Uavg) en het recht om een eigen lezing aan een archiefstuk toe te voegen, in geval van onjuiste persoonsgegevens (art. 45, derde lid, Uavg).

Organisaties dienen verzoeken om inzage in de eigen persoonsgegevens, opgeslagen bij de betreffende organisaties, te beantwoorden aan de verzoeker. Daarvoor kan hetzelfde proces worden doorlopen als bij een standaard informatieverzoek met een wettelijke basis, de terugkoppeling geschiedt dan aan de individuele verzoeker.

6.7 Vernietiging van veiliggestelde e-mail

Het is denkbaar dat veiliggestelde e-mail nog privé-, p-vertrouwelijke of anderszins persoonlijke informatie bevat die niet aan de functie gerelateerd is. Bijvoorbeeld omdat een medewerker niet in de gelegenheid was om binnen tien weken deze te verwijderen. Het is toegestaan om deze e-mails alsnog te vernietigen. Van elke vernietigingsactie dient conform de Archiefwet een verklaring worden opgesteld.

Denk hierbij aan onder meer de volgende informatie: salarisstroken, BSN–nummers, verslagen van personeelsgesprekken, reacties op vacatures, plaatsingsbrieven, burgerbrieven (en reacties hierop) en andere herleidbare gegevens over burgers.

7 Selectie voor blijvende bewaring

Organisaties brengen volgens deze werkwijze e-mail van sleutelfunctionarissen voor permanente bewaring over aan het Nationaal Archief. Dit gebeurt met het oog op de mogelijkheid tot het kunnen reconstrueren van het overheidshandelen op hoofdlijnen op langere termijn (selectiedoelstelling OCW/NA). Naast e-mail van sleutelfunctionarissen kan een organisatie ervoor kiezen om ook andere e-mails over te dragen wanneer zij daar aanleiding toe ziet, bijvoorbeeld betreffende een gebeurtenis die geleid hebben tot opvallende of intensieve interactie tussen overheid en burgers of tussen burgers onderling.

7.1 Sleutelfunctionarissen (ABD Topstructuur)

Het uitgangspunt is dat de topformatie (ABD Topstructuur) als sleutelfunctionaris wordt aangemerkt. Jaarlijks rapporteren en verantwoorden de organisaties de wijzigingen in de topformatie sinds de laatste vaststelling. Dit gebeurt op grond van het Coördinatiebesluit organisatie en bedrijfsvoering rijksdienst van 2011 volgens het daarin genoemde Kader Topstructuur en Topfuncties Rijk 2007.

7.2 Overige sleutelfunctionarissen

Naast deze vooraf vastgestelde groep van topfunctionarissen kunnen organisaties nog andere sleutelfunctionarissen aanwijzen, wanneer deze op basis van een organisatieanalyse een sleutelfunctie binnen de organisatie blijken te vervullen. Voor deze functionarissen geldt dezelfde werkwijze als voor de ABD-topfunctionarissen.

7.3 Register van sleutelfunctionarissen

Het invoeren van de nieuwe werkwijze dient gepaard te gaan met het inrichten van een register van sleutelfunctionarissen per organisatie. Dit register dient alle (in het verleden) aangewezen sleutelfunctionarissen te bevatten. In dit register is minimaal opgenomen:

- Naam en functie van een functionaris;
- Grondslag aanwijzing (ABD of anderszins);
- Organisatieonderdeel;
- Doorlooptijd;
- Op hoofdlijnen, mandaatgebied van de sleutelfunctionaris.

8 Toegang tot veiliggestelde e-mail

8.1 Informatieverzoeken

De veiliggestelde e-mail is in principe toegankelijk voor informatieverzoeken met een wettelijke basis. Dat gaat dan in de regel om WOB-verzoeken, Kamervragen of andere informatie-uitwisseling met de Tweede en Eerste Kamer, recht op inzage conform de AVG, etc..

Organisaties dienen voor het doorzoeken van de veiliggestelde e-mails een aparte regeling vast te stellen. Deze regeling treedt in werking als de gezochte informatie niet via de (oorspronkelijke) eigenaar van de e-mail is te achterhalen. 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.

Toegang tot de veiliggestelde e-mail is strikt beperkt tot de reikwijdte van een specifiek informatieverzoek. Het is daardoor van belang te zorgen voor goede software om het zoekproces te ondersteunen.

8.2 Bedrijfsvoering

Organisaties zijn in eerste instantie slechts gehouden om toegang te verstrekken indien informatieverzoeken met een wettelijke basis aan de orde zijn. Een organisatie kan ook gaan voorzien in het toegankelijk maken van de veiliggestelde e-mail voor de medewerker (alleen eigen e-mail) of ter ondersteuning van de interne bedrijfsvoering. In dit laatste geval selecteert de organisatie, met behulp van software, de e-mails die relevant zijn. Hiervoor geldt dezelfde regeling als voor informatieverzoeken.

9 Overbrengen en openbaar maken van e-mail

E-mail van sleutelfunctionarissen, alsmede eventuele aanvullende e-mail, wordt binnen de daarvoor gestelde termijn in de Archiefwet overgebracht naar het Nationaal Archief. Voor e-mail over gebeurtenissen die geleid hebben tot opvallende of intensieve interactie tussen overheid en burgers, of tussen burgers onderling, zijn per gebeurtenis afspraken te maken.

9.1 Besluit openbaarheid

Bij overbrenging neemt de organisatie conform Archiefwet art. 15, lid 1 een besluit over beperking van de openbaarheid, na advies van de toekomstige beheerder (i.c. de algemene rijksarchivaris). In dat kader kunnen beperkingen aan de openbaarheid worden gesteld op grond van:

- de eerbiediging van de persoonlijke levenssfeer;
- het belang van de Staat of zijn bondgenoten;
- het anderszins voorkomen van onevenredige bevoordeling of benadeling van betrokken natuurlijke personen of rechtspersonen dan wel van derden.

De werkwijze houdt er rekening mee dat een organisatie in het kader van de overbrenging van e-mailbox kan besluiten om de openbaarheid van de betreffende e-mails tijdelijk te beperken. Dit op grond van zowel het voorkomen van onevenredige bevoordeling of benadeling van betrokkenen, als het eerbiedigen van hun persoonlijke levenssfeer.
Het Nationaal Archief gaat uit van een termijn van 25 jaar na creatie, omdat die synchroon is met de termijn voor openbaarheid van vergelijkbaar materiaal, met name de notulen van de ministerraad.

Ten aanzien van de mogelijk aanwezigheid van bijzondere persoonsgegevens en onevenredige benadeling van niet-sleutelfunctionarissen (burgers, ambtenaren, bedrijven) moet, in het kader van een besluit beperking openbaarheid, een beoordeling van de e-mailbox plaatsvinden. Dit kan resulteren in aanvullende beperkingen op de openbaarheid.

9.2 Frequentie van overbrengen

Bij het overbrengen van e-mails van sleutelfunctionarissen naar het Nationaal Archief wordt aangeraden om gebruik te maken van jaarlijkse batches. Dat wil zeggen dat e-mail jaarlijks van een bepaald jaar wordt aangeleverd.

10 Aanpassingen selectielijsten

Het is niet nodig om de geldende selectielijsten bij invoering van de werkwijze aan te passen. Deelnemende organisaties dienen bij het volgen van de handreiking wel een expliciet selectiebesluit vast te stellen (samen met de Minister voor BVOM). De werkwijze voorziet in een generiek model van een selectielijst voor het materiaal dat conform de handreiking Bewaren van e-mail Rijksoverheid is veiliggesteld.

Het generieke selectiebesluit bevat onder meer de volgende bepalingen:

- e-mail van niet-sleutelfunctionarissen krijgt een vernietigingstermijn van tien jaar;
- e-mail van sleutelfunctionarissen wordt blijvend bewaard;
- e-mail wordt, ongeacht functie, bij vaststelling van een gebeurtenis die heeft geleid tot opvallende of intensieve interactie tussen overheid en burgers of tussen burgers onderling (op basis van Archiefbesluit art. 5 lid 1 onder e) uitgezonderd van vernietiging.

Dit is een uitgave van:

Rijksprogramma Duurzaam Digitale
Informatiehuishouding (RDDI)

Februari 2020