Privacy Impact Assessment
E-mailarchivering

Rijksprogramma
Duurzaam
Digitale
Informatiehuishouding

Inhoud

Inleiding 5

A. Beschrijving kenmerken gegevensverwerkingen 7

1. **Voorstel** 7

2. **Persoonsgegevens** 9

3. **Gegevensverwerkingen** 9
   Creatie en opslag 10
   Informatieverzoeken 11
   Recht op inzage 12
   Vernietigen van e-mail 13
   Overbrengen Nationaal Archief 14
   Openbaarmaking 15

4. **Verwerkingsdoeleinden** 16

5. **Betrokken partijen** 16
   Creatie en opslag 16
   Informatieverzoeken 16
   Recht op inzage 17
   Vernietigen van e-mail 17
   Overbrengen Nationaal Archief 17
   Openbaarmaking 18

6 **Belangen bij de gegevensverwerkingen** 18

7. **Verwerkingslocaties** 18

8. **Technieken en methoden van de gegevensverwerkingen** 19

9. **Juridisch en beleidsmatig kader** 19
   Juridisch kader 19

10. **Bewaartermijnen** 19

B. Beoordeling rechtmatigheid gegevensverwerkingen 20
Proportionaliteit en minimale gegevensverwerking 21

11. Rechtsgrond 22

12. Bijzondere persoonsgegevens 23

13. Doelbinding 23

14. Noodzaak en evenredigheid 23

15. Rechten van de betrokkene 24

C. Beschrijving en beoordeling risico's voor de betrokkenen 25

16. Risico's 25

D. Beschrijving voorgenomen maatregelen 29

17. Maatregelen 29
Technische maatregelen 29
Organisatorische maatregelen 30
Juridische maatregelen 30
Bepaling risico na extra maatregelen 31

Inleiding

Er zijn te regelmatig politiek gevoelige incidenten met het niet kunnen terugvinden van digitaal opgeslagen overheidsinformatie, zoals recent nog bij VWS ("Ministerie van VWS verwijderde interne mails over 'loktieners'")[1] en VenJ (onderzoekscommissies Oosting naar Teevendeal). Toezichthouders, adviesraden en auditdiensten zijn al geruime tijd kritisch over het gebrekkige digitale beheer van documenten door de overheid.[2]

In de digitale wereld is de hoeveelheid digitale overheidsinformatie extreem gegroeid. Er is een grote business case voor het verbeteren van de digitale informatiehuishouding binnen het Rijk. E-mail is inmiddels de voornaamste vorm van communicatie binnen het Rijk. Ter illustratie: alleen al het aantal verzonden en ontvangen e-mails binnen het Rijk bedraagt naar schatting minstens een miljard per jaar.[3] Dit is een documentenstroom die onvergelijkbaar is met de hoeveelheden documenten in het pre-digitale tijdperk. 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.

In februari 2016 zocht het ministerie van VWS contact met het ministerie van BZK als voorbereiding op de beantwoording van een commissiebrief n.a.v. de uitzending van Argos inzake een Wob-verzoek. Hierbij is de wens uitgesproken te komen tot Rijksbreed beleid op dit thema. Uitgangspunt voor de richtlijn is, met de voorgestelde nieuwe werkwijze, het opslaan, archiveren en terugzoeken van e-mails Rijksbreed te verbeteren.[4]

Er is momenteel veel onduidelijkheid over de procedures rondom het gebruik van e-mail voor informatieverzoeken. De grote hoeveelheden e-mail die de gemiddelde Rijksmedewerker verstuurt en ontvangt maakt het daarnaast bijzonder complex en tijdrovend om de bestaande procedures te volgen, met als risico dat niet voldaan wordt aan de vereisten van de Archiefwet en de Wob. De procedures zijn veelal nog ontworpen in het pre-digitale tijdperk.

Om in deze onduidelijkheid tegemoet te komen heeft het programma Rijk aan Informatie (RAI), in samenwerking met BZK en OCW, een nieuwe werkwijze ontwikkeld voor het beschikbaar stellen van informatie uit e-mails[5].

[1] Financieel Dagblad, 15-10-2015

[2] Raad voor Cultuur en Raad voor het openbaar bestuur, 'Informatie: grondstof met toekomstwaarde', 2008, – Algemene Rekenkamer, 'Informatiehuishouding van het Rijk', 2010 – Erfgoedinspectie (recent): 'Duurzaam duurt het langst', 2014, 'Onvoltooid Digitaal', 2015.

[3] Quick scan impact Wet open overheid (Woo), 13-12-2016

[4] Het gaat alleen om verzonden en ontvangen e-mail, (nog) niet om agenda-items, taken of andere onderdelen

[5] Een e-mail moet worden gezien als een document binnen het kader van de Wob. Het begrip 'document' moet zeer ruim geïnterpreteerd worden. Artikel 1, aanhef en onder a, van de Wob beschrijft een document als 'een schriftelijk stuk of ander materiaal dat gegevens bevat'. De vorm van de informatie – gedrukt of in elektronische vorm – doet niet ter zake. Door de toevoeging 'of andere materiaal dat gegevens bevat', omvat het begrip document een zeer brede categorie informatiedragers. Van de klassieke papieren dossiers, rapporten, nota's, brieven en vergaderstukken tot foto's, films, diskettes, cd(-rom)'s , dvd's, e-mails, internetpagina's en zelfs mogelijk in de toekomst te ontwikkelen media waarmee gegevens kunnen worden opgeslagen en uitgewisseld.

Deze werkwijze maakt het mogelijk om wel te voldoen aan de vereisten van de Archiefwet en de Wob, op een manier die voor individuele ambtenaren eenvoudiger is dan de meeste bestaande werkwijzen[6]. 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. Er wordt ook wel gesproken van een paradigmashift in de informatiehuishouding.
In de voorgestelde nieuwe werkwijze worden e-mails voor een bepaalde periode opgeslagen en daarna vernietigd. In alle e-mails komen persoonsgegevens voor. Daardoor is de AVG van toepassing en wordt deze privacy impact assessment (PIA) uitgevoerd. Deze PIA is onderliggend aan de richtlijn. Een PIA is verplicht op rijksbrede kaders of richtlijnen waarbij persoonsgegevens worden bewerkt.

Paradigmashift

Zoals aangegeven is in de digitale wereld de hoeveelheid digitale overheidsinformatie extreem gegroeid.
De huidige situatie is enerzijds volkomen onvergelijkbaar met het papieren tijdperk: er is veel meer informatie, er is veel meer technische complexiteit en er spelen vaker verschillende belangen tegelijkertijd, zoals genoemde publieke verantwoording en de beveiliging van systemen die “anyplace, anytime” 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.

Voor e-mail is de situatie dat het informatiebeheer nog veel via handmatige selectie en beoordeling door medewerkers gebeurt. Dat laatste is, gelet op bijvoorbeeld de aantallen mails, extreem tijdsintensief en kostbaar en het leidt tot het risico dat informatie niet correct of zelfs geheel niet gearchiveerd wordt. Voor de Kamer en het publiek is zo niet duidelijk welke informatie bewaard en vernietigd wordt.
Automatisering van dit handwerk betekent een paradigmashift voor het informatie-beheer: systemen nemen medewerkers werk uit handen dat cruciaal is voor het functioneren van het geheugen van de overheid. Medewerkers hoeven niet meer vooraf zelf te selecteren, maar informatie wordt opgeslagen en later kunnen systemen, via gedefinieerde regels en definities, de noodzakelijke selectie aanbrengen. Deze stap is niet voorzien in de huidige praktijk en regelgeving. Ook kan automatisering ingrijpende gevolgen hebben voor het werkdomein van ambtenaren.
In het programma Rijk aan Informatie is afgesproken de paradigmashift allereerst toe te passen in een nieuw bewaarbeleid voor e-mail van het Rijk, als het meest urgente probleem. Als dit werkt voor e-mail kunnen vergelijkbare concepten worden uitgewerkt voor andere informatiedragers.

[6] De voorgestelde methode is gebaseerd op een ontwerp van de National Archives and Records Administration van de VS. Zie ook: https://www.archives.gov/files/records-mgmt/email-management/final-capstone-white-paper.pdf

A. Beschrijving kenmerken gegevensverwerkingen

In hoofdstuk A van deze PIA vindt u een beschrijving van de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

1. Voorstel

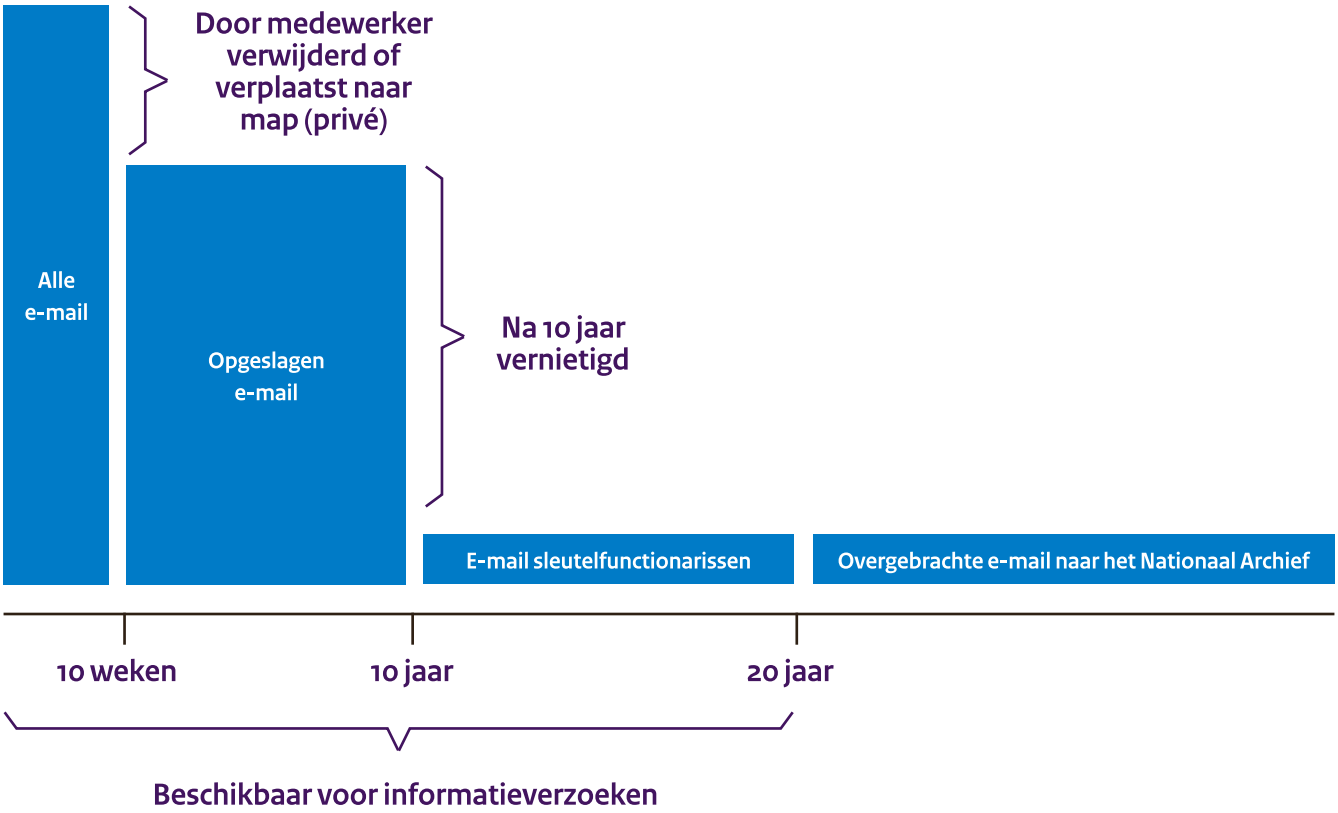
E-mail verzonden of ontvangen door medewerkers van het Rijk wordt, tien weken na creatie of ontvangst, door de ICT dienstverlener[7] automatisch opgeslagen. Medewerkers kunnen in de eerste tien weken privé e-mail, p-vertrouwelijke zaken of andere, niet archiefwaardige e-mail, verwijderen of in een zelf aangemaakt map [prive] in de eigen e-mailomgeving verplaatsen. De overige e-mail wordt tien jaar opgeslagen, waarna deze wordt vernietigd.

Voor te benoemen sleutelfunctionarissen wordt de e-mail permanent bewaard. Na uiterlijk 20 jaar, of zoveel eerder als ministeries beslissen, wordt e-mail van sleutelfunctionarissen[8] naar het Nationaal Archief overgebracht. Deze wordt openbaar beschikbaar gesteld, mogelijk zijn daar bij openbaarheidsbeperkingen van toepassing die het ministerie kan stellen.

Het verwerken van e-mail op de voorgestelde manier, en met name de vernietiging van de daartoe aangewezen e-mail na tien jaar, moet worden verwerkt in de selectielijsten van de ministeries die deze werkwijze willen toepassen. Ministeries die deze werkwijze toepassen dienen hiertoe bij de eerste reguliere herziening maar uiterlijk binnen tien jaar de selectielijsten aan te passen.

[7] Binnen het Rijk zijn op dit moment meerdere ICT-dienstverleners actief die werkplekken, en dus ook e-mail omgevingen, leveren. Het realiseren van de voorgestelde werkwijze zal decentraal, dus door elke ICT-dienstverlener apart, geregeld worden. Er is dus geen sprake van één centraal e-mail archief voor het hele Rijk.

[8] Sleutelfunctionarissen (SF) zijn gedefinieerd als alle medewerkers vanaf ABD Topstructuur, aangevuld met door het ministerie aangedragen relevante medewerkers
Aanvullingen zijn met kennisname van de desbetreffende medewerker
Aanvullingen zijn met zorg geselecteerd o.b.v. de sleutelpositie in relevante dossiers
Aanvullingen zijn noodzakelijk voor relevantie over te dragen e-mail



Methodiek

Het opslaan en vernietigen van e-mail is een geautomatiseerd proces. Deze methodiek zorgt er voor dat de bewaar- en vernietigingstermijnen voor e-mail van het Rijk eenduidig vast zijn gelegd en worden geautomatiseerd. De medewerker kan nog steeds op normale wijze zijn eigen e-mail gebruiken, ook de na tien weken opgeslagen e-mail.

De op deze wijze opgeslagen e-mail is toegankelijk voor informatieverzoeken met een wettelijke basis[9]. Met behulp van standaard zoek-en-vind software kan bij een informatieverzoek binnen de opgeslagen e-mails worden gezocht. Dit mag uitsluitend door speciaal hiervoor aangewezen medewerkers bij concrete informatieverzoeken.

Ten aanzien van de op deze wijze na tien weken door de werkgever opgeslagen e-mail is verder het gestelde uit de AVG ten aanzien van het recht op inzage van toepassing. Dat betekent dat hiervoor voorzieningen worden getroffen. Elke verwerkingsverantwoordelijke is in beginsel gehouden om te reageren op de verzoeken van betrokkenen (zie ook de stappen onder paragraaf 3, gegevensverwerking).

De wet (art. 45, eerste lid, Uavg) voorziet in enkele specifieke uitzonderingen voor zover het gaat om de verwerking van persoonsgegevens die deel uitmaken van archiefbescheiden die berusten in een archiefbewaarplaats (i.d.z.v art. 1, onder f, Aw). In die gevallen zijn inzage- en verbeteringsrechten (art. 15 en 16 AVG), alsmede het recht op beperking van de verwerking in verband met een betwisting van de juistheid van gegevens (art. 18, eerste lid onder a, AVG) en gegevensoverdraagbaarheid (art. 20 AVG) niet van toepassing.

[9] Denk hierbij onder andere aan Wob, AVG, Tweede of Eerste Kamer, maar ook politie en justitie

2. Persoonsgegevens

Met het opslaan van de e-mails worden ook persoonsgegevens verzameld. Artikel 4 van de AVG definieert persoonsgegevens als: “alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.”

Het ligt in de aard van e-mail dat de inhoud ook bijzondere persoonsgegevens kan bevatten, conform genoemd in artikel 9 van de AVG: “persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.”

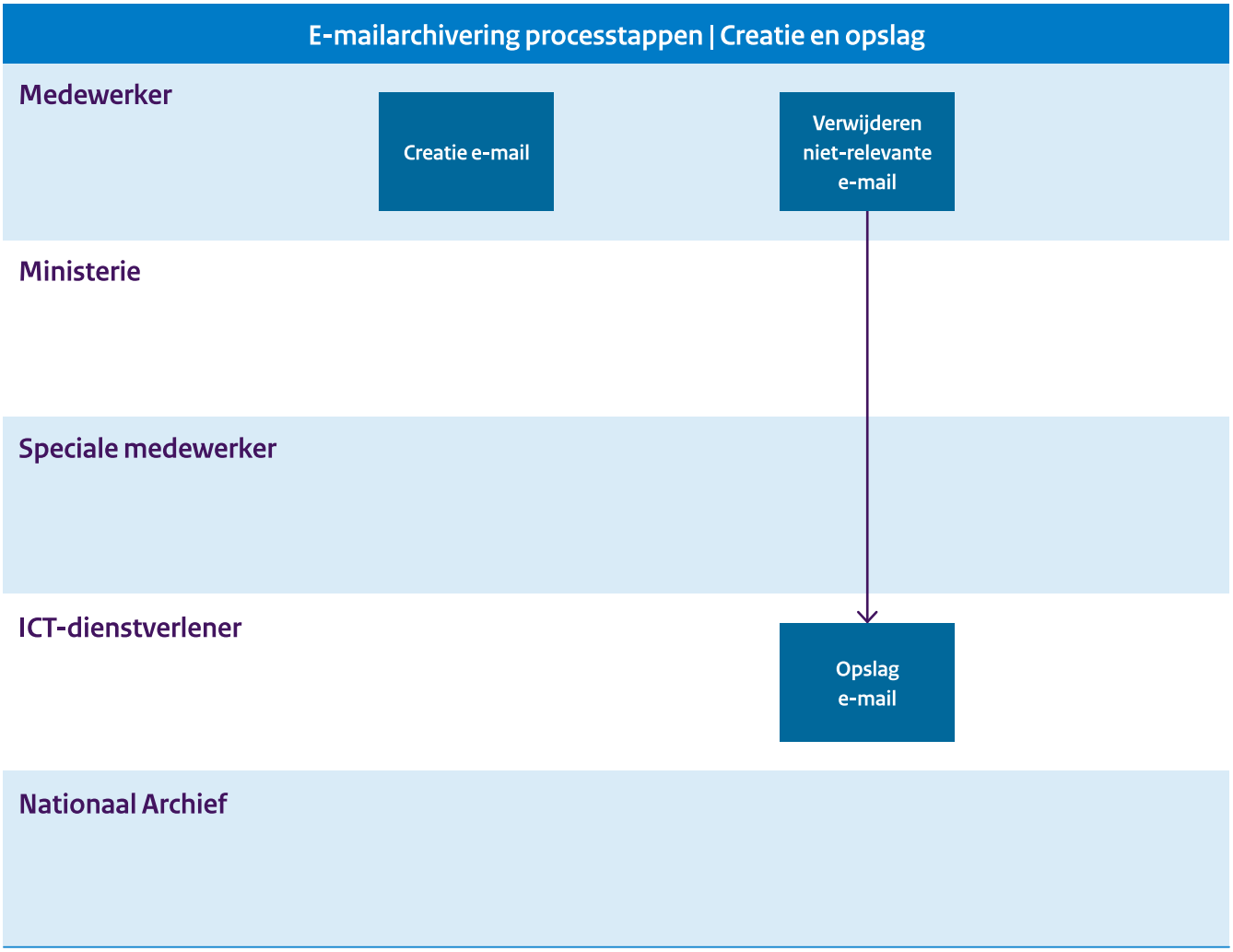
Bovendien bevat de inhoud van e-mails juist de gewenste informatie over bestuurlijke aangelegenheden, waar de overheid zich over dient te verantwoorden conform het wettelijk kader. De betekenis van het begrip ‘bestuurlijke aangelegenheid’ heeft een groot bereik. Een verzoek om informatie betreft een bestuurlijke aangelegenheid als het verband houdt met de beleidsvorming, beleidsvoorbereiding of beleidsuitvoering van een bestuursorgaan. Het woord ‘bestuurlijk’ heeft niet de engere betekenis van ‘administratief’.
Het begrip ‘bestuurlijk’ omvat dan ook niet slechts de uitoefening van bestuurlijke taken en het gebruik van bestuursbevoegdheden, maar heeft betrekking op ‘het functioneren van het openbaar bestuur in al zijn facetten’.
De rechtmatigheid en de grondslag van deze persoonsgegevens is verder uiteengezet in sectie ‘Juridisch en beleidsmatig kader’ van deze PIA.

3. Gegevensverwerkingen

Het proces ten behoeve van opslag en archivering bestaat uit een vijftal hoofdstappen:
- Creatie en opslag
- Informatieverzoek
- Borgen recht op inzage
- Vernietigen van e-mail
- Overbrengen naar Nationaal Archief (NA)
- Openbaarmaking

Deze hoofdstappen worden hieronder elk uitgewerkt.

Creatie en opslag



Creatie e-mail

- e-mail wordt door een medewerker gecreëerd of ontvangen (wordt automatisch opgeslagen in e-mailomgeving [Postvak In] of [verzonden items])

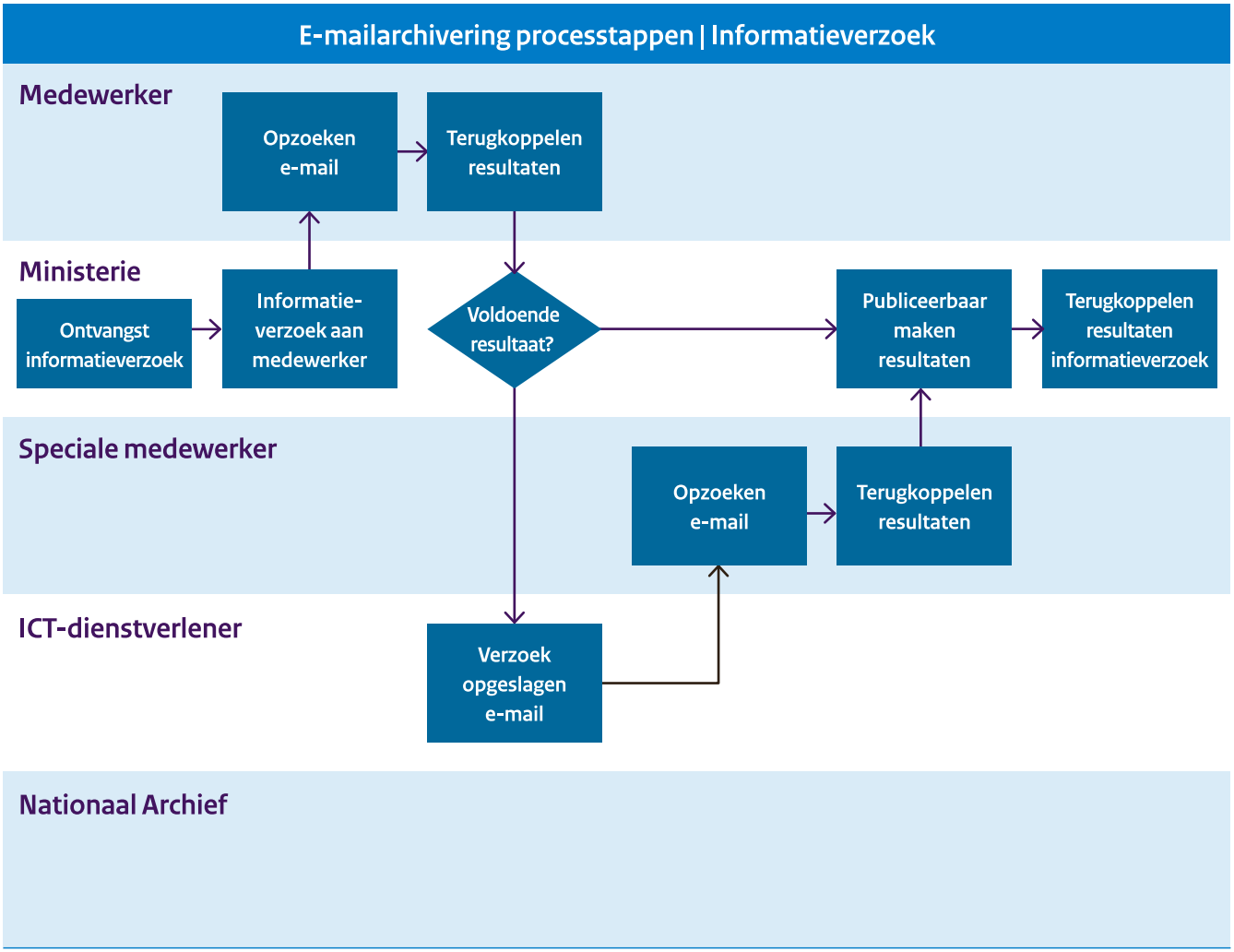
Verwijderen niet-relevante e-mail

- medewerker heeft 10 kalenderweken de tijd om privé e-mail, p-vertrouwelijke zaken of andere, niet archief-waardige e-mail in mapje [prive] te plaatsen of te verwijderen [verwijderde items]

Opslag e-mail

- na 10 kalenderweken wordt e-mail automatisch opgeslagen (of veiliggesteld, afhankelijk van technische oplossing) bij de ICT dienstverlener tbv informatie-verzoeken (uitgezonderd e-mail dat in mapjes [prive] of [verwijderde items] staat)
- de opgeslagen e-mail is alleen toegankelijk voor informatieverzoeken
- na tien weken kan de medewerker e-mail uit eigen e-mailomgeving verplaatsen, verwijderen, etc. zonder dat dit impact heeft op de opgeslagen e-mail

Informatieverzoeken



Ontvangst informatieverzoek
- ministerie krijgt een informatieverzoek binnen

Informatieverzoek aan medewerker
- ministerie vraagt medewerker om e-mails tbv informatieverzoek aan te leveren

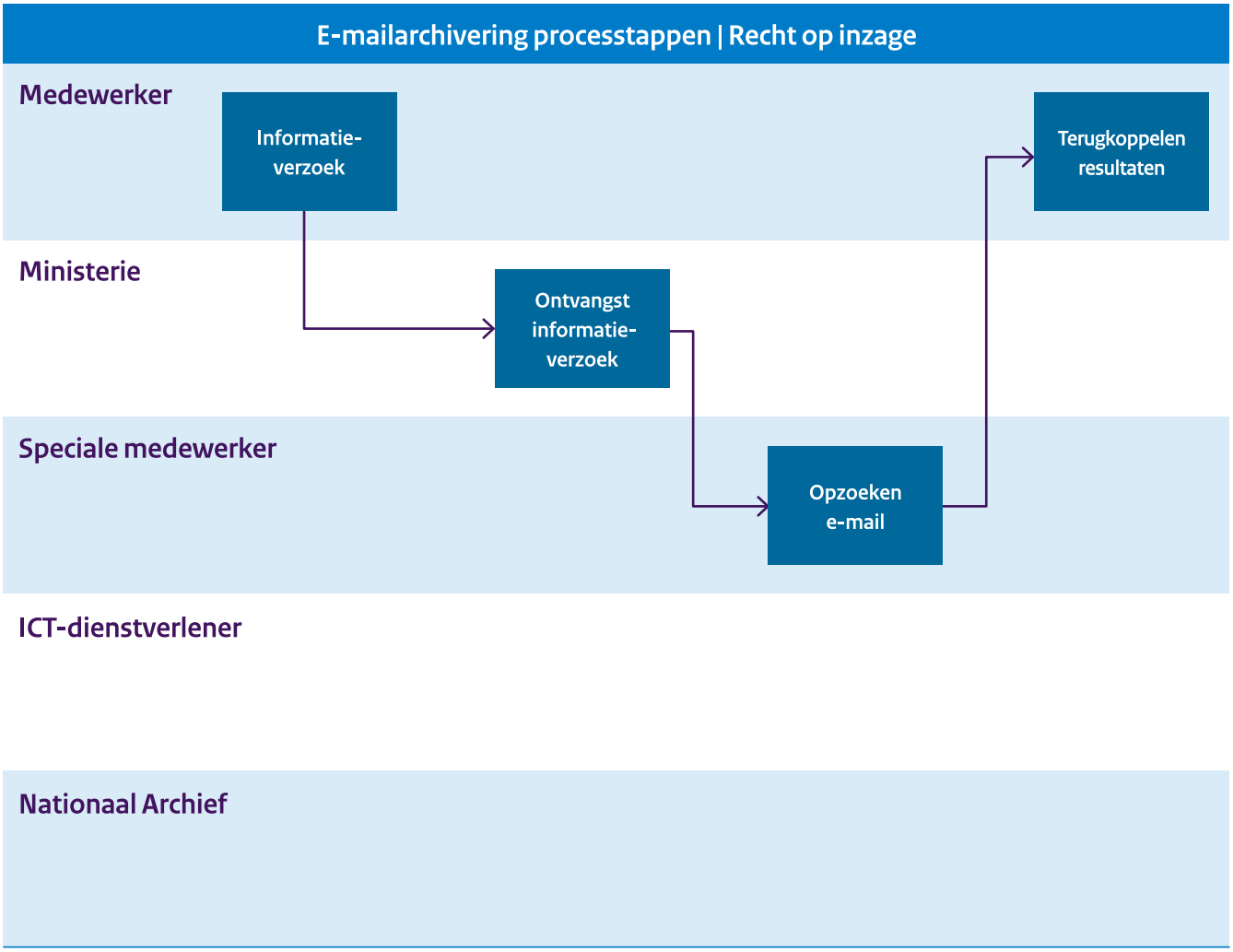
Opzoeken e-mail
- medewerker kijkt in eigen e-mailomgeving

Terugkoppelen resultaten
- medewerker informeert ministerie over resultaat
- <voldoende resultaat?>
- ministerie beoordeelt of resultaat voldoende is
- [nee: resultaat niet voldoende]

Onderzoek opgeslagen e-mail
- indien medewerker gevraagde e-mails niet terug kan vinden, wordt een hier speciaal voor uitgeruste medewerker opdracht gegeven om in de opgeslagen e-mails op zoek te gaan naar de gevraagde e-mails tbv informatieverzoek
- medewerker wordt geïnformeerd
- speciaal uitgeruste medewerker zoekt mbv 'zoek & vind'
- [ja: resultaat voldoende]
- Terugkoppelen resultaten
- speciaal uitgeruste medewerker informeert ministerie over resultaat
- Publiceerbaar maken resultaten
- gevonden e-mails tbv informatieverzoek worden publiceerbaar gemaakt (bv. lakken persoonlijke beleidsopvattingen en persoonsgegevens)[10]
- Terugkoppelen resultaten informatieverzoek gevonden e-mails worden overgedragen tbv informatieverzoek

[10] het Wob kader stelt dat in beginsel geen persoonsgegevens openbaar worden gemaakt, als die er zijn moet een belangenafweging worden gemaakt. Voor zover het persoonlijke beleidsopvattingen van ambtenaren betreft stelt de wet dat die anoniem openbaar kunnen worden als een bewindspersoon dat wenst. Dat kan alleen herleidbaar openbaar worden gemaakt als een medewerker daarmee instemt.

Recht op inzage



Informatieverzoek
- Een medewerker, burger of bedrijf kan een verzoek doen tot inzage

Ontvangst informatieverzoek
- ministerie krijgt een informatieverzoek binnen ten aanzien van inzage van informatie

Opzoeken e-mail
- speciaal uitgeruste medewerker bekijkt in de opgeslagen e-mail naar voorkomende informatie op basis van het verzoek

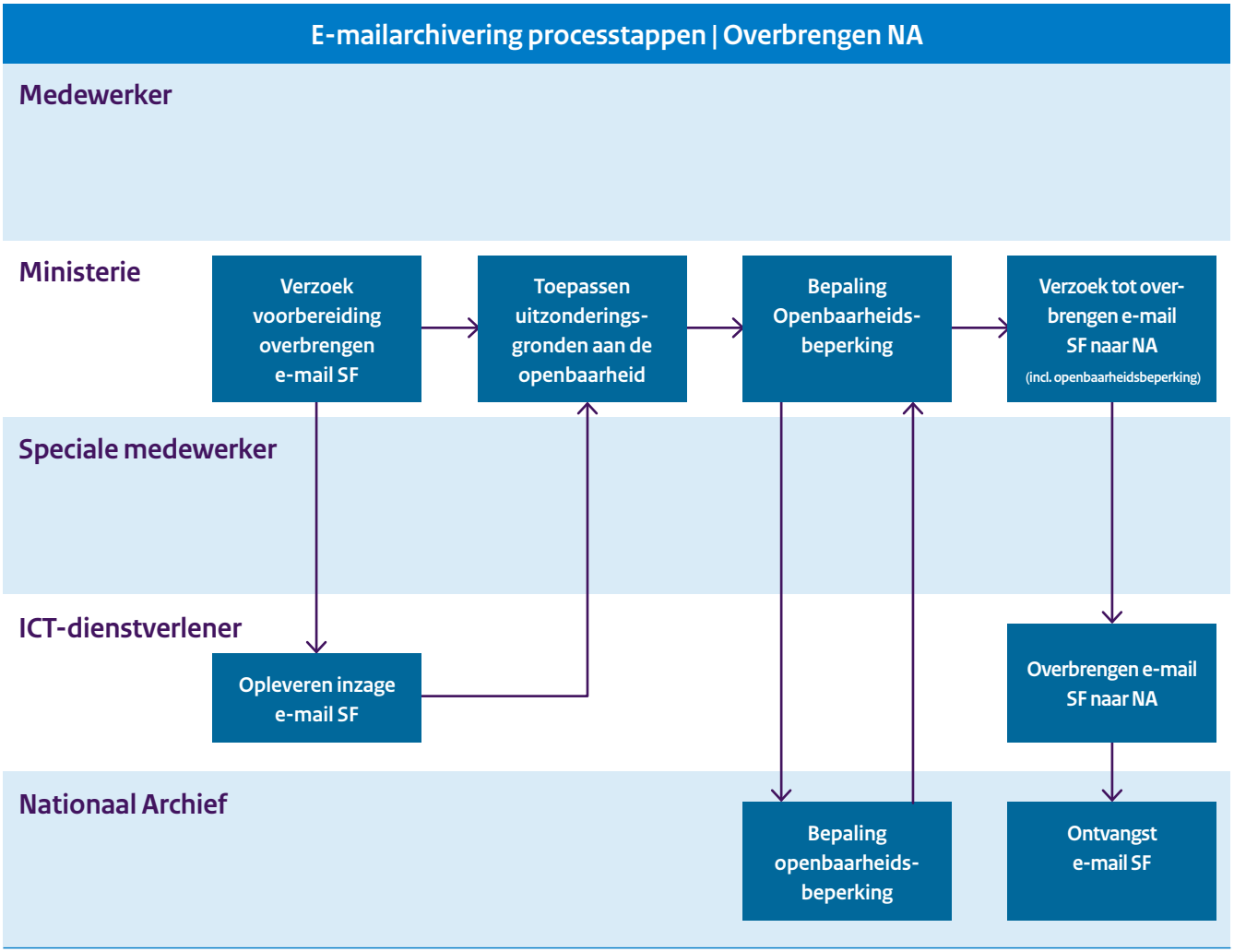
Terugkoppelen resultaten
- Resultaat wordt teruggekoppeld

Vernietigen van e-mail

Vernietigen e-mail niet-SF

- na 10 jaar wordt alle e-mail vernietigd
- inclusief eventuele reserve copy, etc. etc.
- uitgezonderd van vooraf gedefinieerde sleutelfunctionarissen

Overbrengen Nationaal Archief



Verzoek voorbereiding overbrengen e-mail SF
- e-mail van SF'en wordt geanalyseerd ten behoeve van de eventuele toepassing van openbaarheids-beperkingen, in het kader van het voorbereiden op het overbrengen van archiefstukken naar het Nationaal Archief

Opleveren inzage e-mail SF

Toepassen uitzonderingsgronden aan de openbaarheid
- analyse e-mail wordt vertaald naar voorgestelde openbaarheidsbeperking

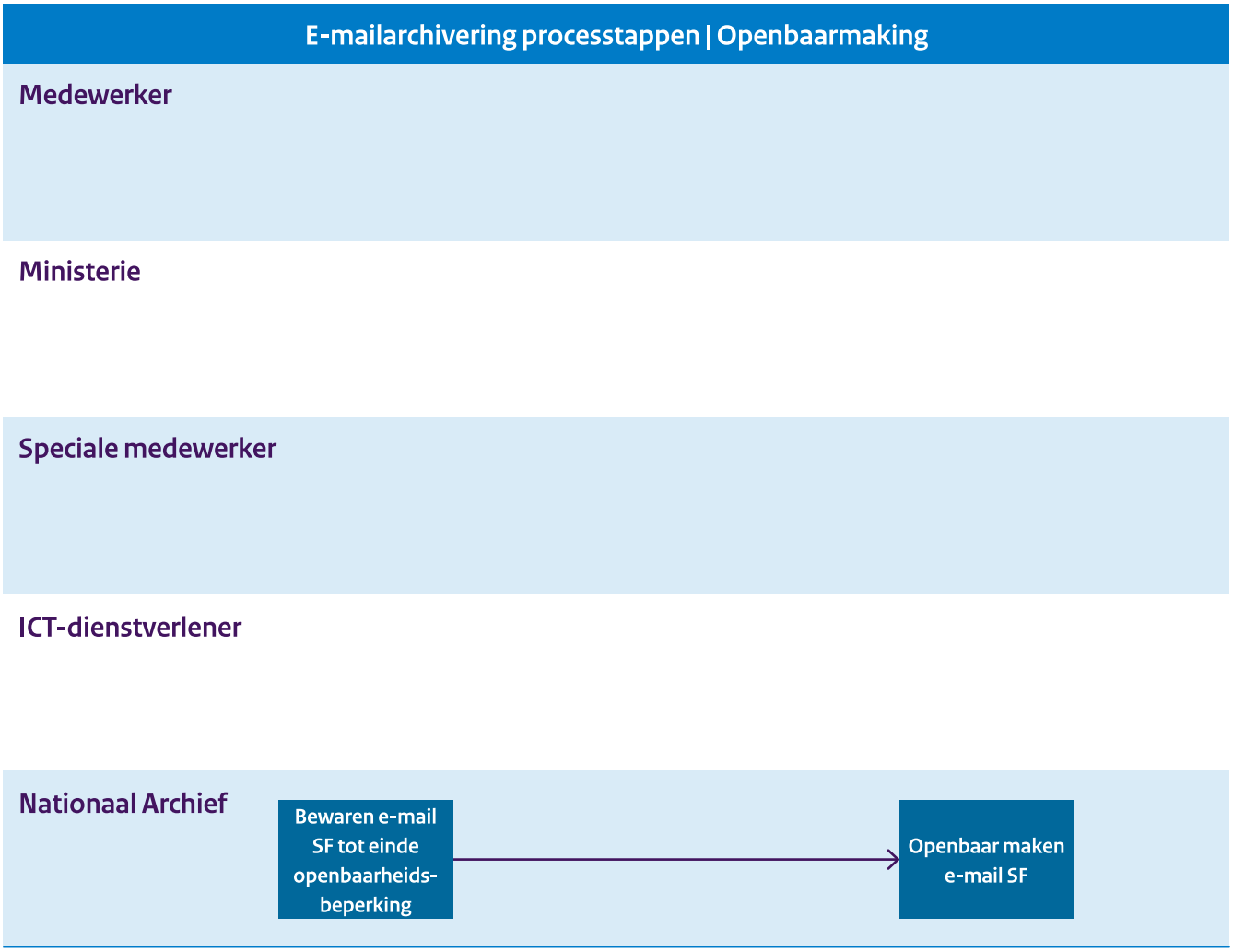
Bepaling openbaarheidsbeperking
- In overleg tussen ministerie en Nationaal Archief wordt de openbaarheidsbeperking vastgesteld

Verzoek tot overbrengen e-mail SF naar NA (incl. openbaarheidsbeperking)

Overbrengen e-mail SF naar NA
- de e-mail van SF'en wordt na 20 jaar overgedragen aan het Nationaal Archief
- conform Archiefwet

Ontvangst e-mail SF

Openbaarmaking



Bewaren e-mail SF tot einde openbaarheidsbeperking

- ontvangen e-mail wordt veilig opgeslagen bij Nationaal Archief, onder voorwaarden is toegang mogelijk voor specifieke onderzoeksdoeleinden overgedragen e-mails worden na einde openbaarheidsbeperking openbaar gemaakt

Openbaar maken e-mail SF

- overgedragen e-mails worden na einde openbaarheids-beperking openbaar gemaakt

4. Verwerkingsdoeleinden

Informatiebeheer bij het Rijk dient van oudsher verschillende doelen. Het goed bewaren van informatie is op korte termijn (informatiehuishouding) nodig voor het eigen functioneren én voor publieke verantwoording (Kamer/WOB). Op de middellange en lange termijn zijn rechtsvinding en (wetenschappelijk) onderzoek de belangrijkste drijfveren (Archiefwet). Archieven zijn daarnaast ook het geheugen van de overheid, dienen ook de publieke verantwoording en vormen uiteindelijk ook cultureel erfgoed.

5. Betrokken partijen

De betrokken partijen zijn per hoofdstap in te delen:

Creatie en opslag

Betrokken organisatie	Verwerkings-verantwoordelijke	Verwerker	Verstrekker	Ontvanger	Functionarissen met toegang tot persoonsgegevens
Kerndepartement	X	X	X	X	Medewerker creëert en heeft toegang tot eigen e-mail
ICT dienstverlener	-	X	-	-	Medewerker met toegang tot e-mailomgeving (niet de inhoud van de e-mail)

Informatieverzoeken

Betrokken organisatie	Verwerkings-verantwoordelijke	Verwerker	Verstrekker	Ontvanger	Functionarissen met toegang tot persoonsgegevens
Kerndepartement	X	X	X	X	Medewerker tot eigen e-mail Speciale medewerker met toegang tot bewaarde e-mail
ICT dienstverlener	-	X	-	-	Medewerker met toegang tot e-mailomgeving (niet de inhoud van de e-mail)

Recht op inzage

Betrokken organisatie	Verwerkings-verantwoordelijke	Verwerker	Verstrekker	Ontvanger	Functionarissen met toegang tot persoonsgegevens
Kerndepartement	X	X	X	X	Medewerker tot eigen e-mail Speciale medewerker met toegang tot bewaarde e-mail
ICT dienstverlener	-	X	-	-	Medewerker met toegang tot e-mailomgeving (niet de inhoud van de e-mail)

Vernietigen van e-mail

Betrokken organisatie	Verwerkings-verantwoordelijke	Verwerker	Verstrekker	Ontvanger	Functionarissen met toegang tot persoonsgegevens
Kerndepartement	X	-	-	-	Op basis van de richtlijn wordt onder verantwoordelijkheid van het ministerie de e-mail na 10 jaar vernietigd
ICT dienstverlener	-	X	-	-	Medewerker met toegang tot e-mailomgeving (niet de inhoud van de e-mail)

Overbrengen Nationaal Archief

Betrokken organisatie	Verwerkings-verantwoordelijke	Verwerker	Verstrekker	Ontvanger	Functionarissen met toegang tot persoonsgegevens
Kerndepartement	X	-	X	-	Op basis van de richtlijn wordt onder verantwoordelijkheid van het ministerie de e-mail na 20 jaar overgebracht
ICT dienstverlener	-	X	-	-	Medewerker met toegang tot e-mailomgeving (niet de inhoud van de e-mail)
Nationaal Archief	-	-	-	X	Medewerker NA

Openbaarmaking

Betrokken organisatie	Verwerkings-verantwoordelijke	Verwerker	Verstrekker	Ontvanger	Functionarissen met toegang tot persoonsgegevens
Nationaal Archief	X	X	-	-	Medewerker NA

6. Belangen bij de gegevensverwerkingen

Het goed bewaren van informatie is op korte termijn (informatiehuishouding) van belang voor het eigen functioneren én voor publieke verantwoording (Kamer/WOB).
Op de middellange en lange termijn zijn rechtsvinding en (wetenschappelijk) onderzoek de belangrijkste drijfveren (Archiefwet). Archieven zijn daarnaast ook het geheugen van de overheid, dienen ook de publieke verantwoording en vormen uiteindelijk ook cultureel erfgoed.
Dit is onder meer vastgelegd in:

- Algemene wet bestuursrecht (Awb): ministerie
- Wet openbaarheid van bestuur (Wob): ministerie
- Archiefwet (Aw): ministerie

Voor de Rijksoverheid is het van groot belang dat kan worden voldaan aan de geschreven en ongeschreven regels met betrekking tot de informatieuitwisseling met TK en EK (volksvertegenwoordiging) en samenleving (waaronder WOB verzoeken). De Rijksoverheid wordt vaak gevraagd zich te verantwoorden over bestuurlijk handelen. Reconstructie hiervan vereist vaak inzage in relevante documentatie zoals nota's, memo's, maar ook zeker relevante e-mails. Zoals in de inleiding is opgenomen in hier vaak discussies over geweest

tussen bewindspersonen en parlement, zoals recentelijk tussen Staatssecretaris VWS en vaste kamercommissie VWS. Hierdoor zal het bewaren van e-mail sterk tegemoet komen aan de vereisten uit de wet en de wens uit de samenleving en parlement.

7. Verwerkingslocaties

Er zijn verschillende dienstverleners actief binnen en buiten het Rijk die e-mail diensten aanbieden aan ministeries of onderdelen daarvan. Er is geen integraal overzicht van waar al deze gegevens worden opgeslagen. Elk ministerie is zelf verantwoordelijk om te voldoen aan de Baseline Informatiebeveiliging Rijk 2017 en andere relevante regelgeving zoals privacyregelgeving.
Het is niet de bedoeling met de nieuwe methode van e-mailarchivering iets te veranderen aan de locaties waar ministeries of andere rijksorganisaties hun e-mail nu laten opslaan.

8. Technieken en methoden van de gegevensverwerkingen

Er is geen sprake van (semi-) geautomatiseerde besluitvorming, profilering of big data-verwerkingen. Gebruik wordt gemaakt van e-mail server en clients om de e-mail te bewaren en bewaartermijnen toe te passen. Er wordt gebruik gemaakt van zoek en vind software om e-mails, waar nodig, terug te vinden. E-mails worden na lange tijd overgebracht naar het e-depot van het Nationaal Archief.

9. Juridisch en beleidsmatig kader

Juridisch kader

Er zijn een aantal wettelijke verplichtingen die op de Minister rusten die hem noodzaken tot een ordentelijke opslag van e-mails. Hierbij moet in hoofdzaak aan de volgende verplichtingen worden gedacht:

1. 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.
2. 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.
3. 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.[11]

Voorafgaand aan dan wel naast de bovengenoemde wettelijke verplichtingen ligt de algemene taak van de minister om transparant te zijn over de uitoefening van publieke taken en daar (desgevraagd) verantwoording over te kunnen afleggen aan de politiek en burgers.

[11] Ten aanzien van de goede geordende en toegankelijke staat van de archieven heeft het miniserie van OCW en het Nationaal Archief bepaald dat de op deze wijze verzamelde e-mail voldoet aan de vereisten uit artikel 3 van de archiefwet.

10. Bewaartermijnen

In deze e-mail werkwijze is gekozen voor vernietiging van e-mail archieven van niet sleutelfunctionarissen na een termijn van tien jaar om verantwoording van overheidshandelen op middellange termijn goed te borgen. Daarnaast is deze termijn goed toepasbaar in relatie tot de gangbare vernietigingstermijnen van het merendeel van de overheidsinformatie. Deze termijn is voorgesteld op aangeven van het CIO-beraad. Korter zou geen recht doen aan nog lopende dossiers, die kunnen bijvoorbeeld bij infrastructurele werken tien jaar in ontwikkeling zijn. E-mail van sleutelfunctionarissen wordt permanent bewaard, daarmee is continuïteit en verantwoording ook geborgd na tien jaar, alsmede de overdracht van relevante informatie aan het Nationaal Archief.

Vernietigen van overheidsdocumenten vindt op grond van de Archiefwet plaats op basis van selectielijsten. Deze leggen vast voor verschillende soorten van informatie wat de bewaartermijn is. Selectielijsten kennen (vele) verschillende vormen van bewaartermijnen, die veelal zijn ontleend aan wettelijke bewaartermijnen. In deze e-mail werkwijze is gekozen voor vernietiging na een termijn van tien jaar om verantwoording van overheidshandelen op middellange termijn goed te borgen. Daarnaast is deze termijn goed toepasbaar in relatie tot de gangbare vernietigingstermijnen van het merendeel van de overheidsinformatie.

Het verwerken van e-mail op de voorgestelde manier, en met name de vernietiging van de daartoe aangewezen e-mail na tien jaar, moet worden verwerkt in de selectielijsten van de ministeries die deze werkwijze willen toepassen. Ministeries die deze werkwijze toepassen dienen hiertoe bij de eerste reguliere herziening maar uiterlijk binnen tien jaar de selectielijsten aan te passen.

Hierbij moet worden opgemerkt dat een klein deel van de gegevens permanent zal worden bewaard. Het gaat hier om de gegevens van te benoemen sleutelfunctionarissen. Deze gegevens worden als relevant geacht voor cultuur en historisch onderzoek in het kader van de Archiefwet. Archieven zijn daarnaast ook het geheugen van de overheid, dienen ook de publieke verantwoording en vormen uiteindelijk ook cultureel erfgoed.

B. Beoordeling rechtmatigheid gegevensverwerkingen

In dit hoofdstuk beoordelen wij de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene.

Wij beoordelen aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond,noodzaak en doelbinding van de gegevensverwerkingen. Wij beoordelen tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen.

Het is allereerst goed om in herinnering te brengen dat deze PIA niet ziet op het verzenden en ontvangen van e-mails en het "lokaal" opslaan van verzonden en ontvangen e-mails op de account van de betreffende medewerker. Deze PIA ziet enkel op de opslag van bepaalde verzonden en ontvangen e-mails op een centrale omgeving. De opslag op de centrale omgeving kwalificeert als een verdere verwerking. "Verdere verwerking ziet in de verordening op verwerkingen van persoonsgegevens voor een ander doel dan waarvoor de persoonsgegevens oorspronkelijk zijn verzameld." (Kamerstukken II 2017/18, 34 851, nr. 3, p. 37).

Een verdere verwerking wordt onder de AVG toegestaan in een drietal situaties (artikel 6, vierde lid):
1. indien er sprake is van een verenigbaar doel;
2. indien de betrokkene toestemming voor de verdere verwerking heeft gegeven;
3. op basis van een Unierechtelijke of lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in artikel 23, eerste lid, van de verordening bedoelde doelstellingen van algemeen belang.

De verdere verwerking met het oog op archivering in het algemeen belang wordt overeenkomstig artikel 89, eerste lid, van de AVG niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd. (artikel 5, eerste lid, onder b, overweging 50 en Kamerstukken II 2017/18, 34 851, nr. 3, p. 38).

In het onderhavige geval is de verdere verwerking met het oog op archivering in het algemeen belang en daarmee dus verenigbaar met het oorspronkelijke doel van de verwerking. Ten aanzien van vaststelling van de grondslag geldt dan:

"Als kan worden vastgesteld dat er sprake is van een verenigbaar doel, is voor de verdere verwerking geen andere afzonderlijke rechtsgrond vereist dan die op grond waarvan de verzameling van de persoonsgegevens werd toegestaan. De Unierechtelijke of lidstatelijke bepaling die als rechtsgrond voor de verwerking van persoonsgegevens dient, kan ook dienen als rechtsgrond voor de verdere verwerking voor een verenigbaar doel. Dit geldt voor alle verwerkingsverantwoordelijken, derhalve ook voor overheidsinstanties. Er is geen reden om aan te nemen dat in geval van overheidsinstanties er altijd een specifieke grondslag moet zijn voor verdere verwerking, als het gaat om een doel dat verenigbaar is met het oorspronkelijke doel." (*Kamerstukken II* 2017/18, 34 851, nr. 3, p. 38).

Proportionaliteit en minimale gegevensverwerking

De proportionaliteit en minimale gegevensverwerking zijn getoetst bij advocatenkantoor Brinkhof. Gerrit-Jan Zwenne (beëdigd in 1998) is per 1 februari 2016 als partner verbonden aan Brinkhof. Hij is gespecialiseerd in privacy-, telecom- en internetrecht. Daarnaast is Gerrit-Jan hoogleraar recht en de informatiemaatschappij aan de Universiteit Leiden.
"De Rijksoverheid kan zich op het standpunt stellen dat het nieuwe bewaarbeleid zich goed verdraagt met de vereisten van rechtmatigheid, behoorlijkheid en transparantie, alsmede van doelbinding (art. 5, eerste lid, onder *a* resp. *b*, AVG)."

"[Voor] de Rijksoverheid [is] de verwerking in het kader van het bewaarbeleid noodzakelijk, ofwel ter naleving van wettelijke verplichtingen die op de desbetreffende verwerkingsverantwoordelijke (op rijksniveau: de minister)[12] rust, ofwel voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen (art. 6 lid 1 onder *c* resp. *e* AVG).

Waar het gaat om het bewaren 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' (overw. 50 AVG). Verder geldt de verplichting van artikel 3 Aw. Op grond daarvan wordt van overheidsorganen verlangd dat zij de onder hen berustende archiefbescheiden in goede, geordende en toegankelijke staat brengen en bewaren. Waar het gaat om het opzoeken, doorzoeken en beschikbaar stellen van bewaarde e-mail moet in elk geval worden gedacht aan de verplichtingen om uit eigen beweging of op verzoek informatie over bestuurlijke aangelegenheden openbaar te maken (art. 3 en 8 Wob), alsmede aan de verplichting van de minister om de door leden van de Tweede en Eerste Kamer verlangde inlichtingen te verstrekken.

De beide verwerkingsgrondslagen stellen als voorwaarde dat de desbetreffende verwerkingen noodzakelijk zijn voor het naleven van de wettelijke verplichting respectievelijk de taak van algemeen belang of uitoefening van openbaar gezag. Dit betekent dat er niet meer moet worden bewaard dan daarvoor nodig is. In termen van rechtmatigheid en behoorlijkheid (art. 5, eerste lid, onder *a*, AVG) wordt dit onder andere geborgd doordat de desbetreffende ambtenaar gedurende tien weken in de gelegenheid wordt gesteld om zelf de e-mailberichten te verwijderen die naar zijn oordeel voor de naleving van de wettelijke plicht of de taak van algemeen belang onnodig zijn. Voorstelbaar is nog dat er functionaliteiten worden ontwikkeld die het gemakkelijk maken om e-mailberichten te verwijderen, door bijvoorbeeld e-mails als zodanig te markeren."

"In termen van **doelbinding** (art. 5, eerste lid, onder *b*, AVG) is er weliswaar sprake van een verdere verwerking, echter deze zal in beginsel niet als onverenigbaar met het verzameldoel worden aangemerkt.[13] Daarbij komt uiteraard betekenis toe aan de opmerkingen gemaakt in de preambule van de AVG (overw. 50) en de tweede zin van de desbetreffende bepaling (art. 5, eerste lid, onder b, AVG) over archivering, namelijk dat:
"de verdere verwerking met het oog op archivering in het algemeen belang, [..] wordt niet als onverenigbaar de oorspronkelijke doeleinden beschouwd."

[12] Zie over voor de kwalificatie van de «de verantwoordelijke» (en het daarmee overeenstemmende begrip «verwerkingsverantwoordelijke») op rijksniveau: Kamerstukken II 1997/98, 25 892, nr. 3, p.
[13] Kamerstukken II 2017/18, 34 851, nr. 3, p. 37.

Evenals bij de vereisten met betrekking tot rechtmatigheid en behoorlijkheid (art. 5, eerste lid, onder *a*, AVG) is van belang dat er wordt geborgd dat er niet teveel (want niet voor de naleving van wettelijke plichten en/of taak van algemeen belang relevante) e-mailberichten worden bewaard. En daarvoor is dan weer van belang dat de desbetreffende ambtenaar binnen de tien wekentermijn zelf de berichten kan uitzonderen die naar zijn oordeel niet relevant zijn.

Voor de doelbinding is verder relevant dat de mogelijke gevolgen voor de betrokkenen (d.w.z. de desbetreffende ambtenaar en anderen) van het bewaren 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 ambtenaar worden afgewogen tegen het belang bij openbaarmaking (bijv. o.g.v. art. 10, eerste lid, onder d resp. tweede lid, onder e, Wob of art. 15, eerste lid, onder a, Aw). Oftewel, als e-mailberichten gedurende tien jaar, en in geval van sleutelfunctionarissen permanent, worden bewaard is daarmee niet gezegd dat daarmee de persoonlijke levenssfeer van de desbetreffende ambtenaar (of anderen over wie het bericht persoonsgegevens bevat) wordt aangetast, en als dat zou gebeuren, dan alleen na een belangenafweging."
"Ook waar het gaat om het beginsel van *privacy-by-design* (art. 25, eerste lid, AVG) lijkt het bewaarbeleid te voldoen aan de gestelde vereisten. Wél komt daarbij meer betekenis toe aan de functionaliteiten waarmee het voor de ambtenaar gemakkelijker wordt om irrelevante e-mailberichten te kunnen uitsluiten. Het zijn dergelijke functionaliteiten (of *tools*) die, gelet op de doeleinden waarvoor de gegevens worden verwerkt, eraan bijdragen dat aan de vereisten van de verordening wordt voldaan. "

11. Rechtsgrond

Ingevolge artikel 6 van de AVG is een gegevensverwerking alleen rechtmatig indien aan ten minste een van de onderstaande voorwaarden is voldaan:

a. de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Gelet op het vorenstaande is in het onderhavige geval geen afzonderlijke rechtsgrond vereist. Dat laat onverlet dat er wel grondslagen zouden zijn waarop de verwerking gebaseerd kan worden, namelijk onder gronden c en e. De wettelijke verplichtingen en publieke taken zijn uitgewerkt onder 9 en 14.

12. Bijzondere persoonsgegevens

Artikel 9 van de verordening ziet op verwerking van bijzondere categorieën van persoonsgegevens. Uitgangspunt is dat verwerking van bijzondere categorieën van persoonsgegevens verboden is, tenzij een van de in uitzonderingen zich voordoet. In het onderhavige geval is de uitzondering genoemd onder artikel 9, tweede lid, onder j, aan de orde: de verwerking is noodzakelijk met het oog op archivering in het algemeen belang.

13. Doelbinding

Zoals hierboven geconstateerd is sprake van een verdere verwerking. Het oorspronkelijke doel van de gegevensverwerking is het versturen en ontvangen van elektronische berichten. De verzonden en ontvangen berichten worden lokaal opgeslagen voor het eigen archief van de medewerker. De centrale opslag ziet op een specifieke archieffunctie in het kader van verantwoording en transparantie.

Het doel van de verdere verwerking valt binnen hetgeen de verordening verstaat onder archivering in het algemeen belang: “Overheidsinstanties (...) die in het bezit zijn van gegevens van algemeen belang moeten diensten zijn die, conform het Unierecht of het lidstatelijke recht, wettelijk verplicht zijn gegevens van blijvende waarde voor het algemeen belang te verwerven, te bewaren, te beoordelen, te ordenen, te beschrijven, mee te delen, onder de aandacht te brengen, te verspreiden en toegankelijk te maken. De lidstaten moeten tevens worden gemachtigd om te bepalen dat persoonsgegevens voor archiveringsdoeleinden verder mogen worden verwerkt, bijvoorbeeld met het oog op het verstrekken van specifieke informatie over het politiek gedrag onder voormalige totalitaire regimes, over genocide, misdaden tegen de menselijkheid, met name de Holocaust, of over oorlogsmisdaden.” (overweging 158)

Voor wat betreft de doelbinding wordt verder verwezen naar hetgeen onder B staat.

14. Noodzaak en evenredigheid

Het is om uiteenlopende redenen steeds moeilijker om aan voormelde wettelijke verplichtingen te voldoen.
Dit komt onder meer door:

- de toenemende omvang van het gebruik van e-mails op de werkvloer;
- een onhandig en zeer tijdrovend proces voor medewerkers;
- het beleid dat de individuele medewerker zelf actie moeten ondernemen voor de archivering;
- onduidelijke en multi-interpretabele regelgeving.

De redenering achter de beoogde richtlijn is dat gegeven deze omstandigheden onvoldoende uitvoering kan worden gegeven met de huidige werkwijze aan bovenvermelde wettelijke verplichtingen en dat de nieuwe werkwijze daar verandering in brengt. Uit het oogpunt van proportionaliteit is een aantal alternatieven afgewogen waaruit de nieuwe werkwijze naar voren is gekomen. Volledigheidshalve zijn hieronder de afgewogen alternatieven opgenomen:

Huidige methode in stand houden; medewerker archiveert zelf (in DMS, of ander opslagmedium)
De huidige regelgeving is multi-interpretabel en tevens onhandig en tijdrovend voor medewerkers. Het gaat om grote volumes e-mail. Vaak vele honderden per week.
De toepassing van het systeem van selectielijsten door medewerkers, gekoppeld aan de actie om e-mail zelf veilig te stellen op de juist plek in een DMS leidt tot zeer tijdrovende en intensieve processen die veelal niet worden toegepast. Het is ook redelijkerwijs niet te verwachten dat organisaties deze werkwijze wel volledig naleven, de werkbelasting op organisaties wordt te groot om te verwachten dat alle e-mail individueel wordt gearchiveerd. Ten slotte is nog op te merken dat in de digitale wereld niet verwacht hoeft te worden dat e-mails handmatig gearchiveerd hoeven worden. Dat kan ook op meer automatische wijze.

E-mail wordt na een bepaalde periode verwijderd, dient in DMS te worden bewaard
Hierbij worden medewerkers gedwongen om volgens de huidige methode te gaan werken. De belasting voor medewerkers blijft, zoals bij 1., zeer groot. Daarbij is het terugzoeken van e-mail een nog intensiever proces, het is niet meer in de e-mail-omgeving terug te vinden, alleen in het DMS.

Medewerker markeert e-mail in mailbox, wordt dan automatisch opgeslagen (archive knop), eventueel met metadata velden
Deze methode is meer automatisch dan het overzetten naar een DMS, wel wordt op elke archiefwaardige e-mail actie verwacht van medewerkers, wat nog steeds een grote belasting en onbegrip met zich mee brengt. In de beoogde werkwijze wordt in principe geen of weinig actie gevraagd (slechts bij privé mail).

DIV medewerkers e-mail laten archiveren
Individuele selectie en waardering zal, ook al gebeurt dat door gespecialiseerde medewerkers, een zeer grote belasting met zich meebrengen.

Back-ups gebruiken voor e-mail terugzoeken, (selectie daarvan) overdragen aan Nationaal Archief
In back-ups wordt alles opgeslagen, het streven van de beoogde methode is medewerkers nog enige controle te geven privé mail aan de opslag te onttrekken. Tevens zijn back-ups technisch niet aan te raden als volwaardig archief. Bij een eventuele migratie van dienstverlener of technische omgeving is het niet te garanderen dat een oudere back-up in een nieuw systeem kan worden uitgelezen. Back-ups zijn ook niet ingericht voor informatieverzoeken, het zijn momentopnames en als er iets moet worden terug gezocht moet handmatig een specifiek deel van de back-up op een apart medium worden gezet.

Centrale mailbox die wordt gearchiveerd waar relevante mails heen worden gezonden
Ook hier wordt van medewerkers een handmatig proces per e-mail verwacht, wat een grote belasting met zich meebrengt.

Zero mail (of iig geen beslissingen over de mail)
Het is een te grote stap om te verwachten dat e-mail binnen enkele jaren niet meer gebruikt wordt binnen het Rijk.

15. Rechten van de betrokkene

In de voorgenomen nieuwe werkwijze gaat het alleen om het aanpassen van de bewaartermijnen van e-mail en het permanent bewaren van een selectie die relevant kan zijn voor historisch onderzoek zoals bedoeld in de archiefwet. Het is niet de bedoeling aanpassingen te maken aan de rechten van betrokkenen op welke wijze dan ook ten aanzien van het gebruik van e-mail binnen het Rijk.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Wij hebben aan de hand van de feiten zoals vastgesteld in onderdeel A bepaald dat de voorgenomen gegevensverwerkingen rechtmatig zijn (in onderdeel B). Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Wij hebben tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen als rechtmatig beoordeeld. In dit hoofdstuk beschrijven en beoordelen wij de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Hierbij houden wij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerking. Dit zijn de gegevensverwerkingen zoals in onderdeel A en B beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's

Voor de Rijksoverheid is het van groot belang dat kan worden voldaan aan de geschreven en ongeschreven regels met betrekking tot de informatie-uitwisseling met TK en EK (volksvertegenwoordiging) en samenleving (waaronder WOB verzoeken). De Rijksoverheid wordt vaak gevraagd zich te verantwoorden over bestuurlijk handelen. Reconstructie hiervan vereist vaak inzage in relevante documentatie zoals nota's, memo's, maar ook zeker relevante e-mails.

Het is om uiteenlopende redenen steeds moeilijker om aan voormelde wettelijke verplichtingen te voldoen. De redenering achter de beoogde richtlijn is dat gegeven deze omstandigheden onvoldoende uitvoering kan worden gegeven met de huidige werkwijze aan bovenvermelde wettelijke verplichtingen en dat de nieuwe werkwijze daar verandering in brengt. Uit het oogpunt van proportionaliteit is een aantal alternatieven afgewogen waaruit de nieuwe werkwijze naar voren is gekomen. Het bewaren van e-mail zal sterk tegemoet komen aan de vereisten uit de wet en de wens uit de samenleving en parlement.

In de voorgenomen nieuwe werkwijze gaat het alleen om het aanpassen van de bewaartermijnen van e-mail en het permanent bewaren van een selectie die relevant kan zijn voor historisch onderzoek zoals bedoeld in de archiefwet. Het is niet de bedoeling aanpassingen te maken aan de rechten van betrokkenen op welke wijze dan ook ten aanzien van het gebruik van e-mail binnen het Rijk. Er is geen sprake van (semi-) geautomatiseerde besluitvorming, profilering of big data-verwerkingen. In de nieuwe methode worden e-mails opgeslagen. Met het opslaan van de e-mails worden ook persoonsgegevens verzameld, bijvoorbeeld het e-mailadres. E-mail is een laagdrempelig communicatiemiddel. Het ligt in de aard van e-mail dat de inhoud ook bijzondere persoonsgegevens kan bevatten. Dit kunnen zowel persoonsgegevens zijn van medewerkers, als ook van burgers en bedrijven. Door de aanwezigheid van persoonsgegevens is de nieuwe methode potentieel een risico op de privacy van de betrokkenen.

Deze risico's zijn in te delen in een tiental soorten:
1. Risico op inbreuk op de persoonlijke levenssfeer
2. Risico op aanzienlijk economisch of maatschappelijk nadeel
3. Risico op inbreuk op de bescherming van de lichamelijke integriteit
4. Risico op onrechtvaardige behandeling
5. Risico op ongelijke behandeling
6. Risico op aantasting van de autonomie
7. Risico op beschadiging van reputatie

8. Risico's voor de veiligheid van de respondent en/of zijn familie
9. Risico op aantasting menselijke waardigheid
10. Risico's voor bescherming overige (grond)rechten

Het risico is te bepalen door de kans van optreden te meten aan de impact (risico = kans x impact).

- Kans: kans op optreden van een risico
- Impact: effect wanneer het risico optreedt

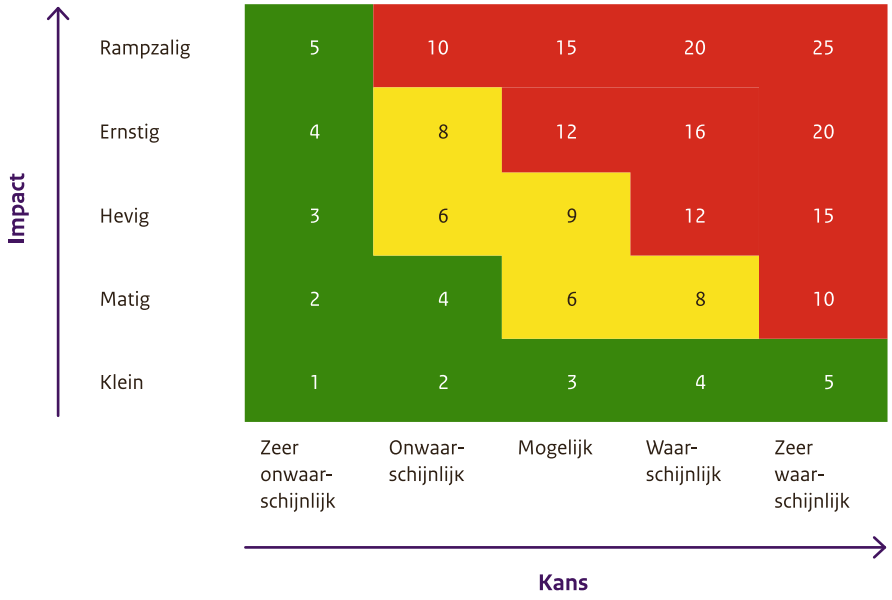
Zowel de kans als de impact wordt geclassificeerd. Het risico wordt vervolgens uitgedrukt in een getal en gevisualiseerd in een tolerantiematrix.

De tolerantiematrix bestaat uit drie zones: groen, geel en rood. Onderstaande matrix geeft schematisch weer wanneer bij welke uitkomst er aanvullende maatregelen getroffen dienen te worden. Dit is zeker het geval bij de rode zone, maar kan in het kader van privacy ook voor de gele zone worden verwacht. Uiteindelijk zal per risico moeten worden bepaald hoe met de betreffende risico omgegaan wordt. De inschatting van kans en impact is altijd subjectief en een inschatting is gebaseerd op de beschikbare informatie.

In deze PIA wordt uitgegaan van onderstaande tolerantiematrix en zones:

Tolerantiematrix

Figuur 1: https://www.house-of-control.nl/risicomanagement-risicoanalyse-risicomanagementsysteem-tolerantiematrix-maatregelen.html



Hieronder geven wij in een tabel aan hoe wij de risico's inschatten.

nr.	Risico	Impact	Kans	Risicozone
1.	Risico op inbreuk op de persoonlijke levenssfeer	Ernstig	Onwaarschijnlijk	Geel
2.	Risico op aanzienlijk economisch of maatschappelijk nadeel	Matig	Onwaarschijnlijk	Groen
3.	Risico op inbreuk op de bescherming van de lichamelijke integriteit	Klein	Onwaarschijnlijk	Groen
4.	Risico op onrechtvaardige behandeling	Matig	Onwaarschijnlijk	Groen
5.	Risico op ongelijke behandeling	Matig	Onwaarschijnlijk	Groen
6.	Risico op aantasting van de autonomie	Matig	Onwaarschijnlijk	Groen
7.	Risico op beschadiging van reputatie	Ernstig	Onwaarschijnlijk	Geel
8.	Risico's voor de veiligheid van de respondent en/of zijn familie	Matig	Onwaarschijnlijk	Groen
9.	Risico op aantasting menselijke waardigheid	Matig	Onwaarschijnlijk	Groen
10.	Risico's voor bescherming overige (grond)rechten	Ernstig	Onwaarschijnlijk	Geel

De kans dat een risico optreedt is ingeschat als 'onwaarschijnlijk'. Dit is een voorzichtige inschatting, gebaseerd op de huidige maatregelen en het aantal geconstateerde incidenten op de beveiliging van de overheidsdata. De beveiliging van de opslag van deze gegevens is altijd onderhavig aan de vereisten vanuit de informatiebeveiliging van het Rijk (de baseline informatiebeveiliging Rijk 2017).

Daarnaast is het goed om te beseffen dat het voorstel een nieuwe werkwijze is. Het voorstel verandert niets aan de voorwaarden waaronder iets openbaar wordt. De nieuwe werkwijze gaat gebruik maken van dezelfde beveiliging. Het risico dat in de e-mails zaken staan die compromitterend zijn of op een of andere manier een reputatie kunnen beschadigen, worden wellicht voor het gevoel groter met deze nieuwe werkwijze. Er wordt nu ook al op grote schaal informatie opgeslagen en e-mails vallen nu ook al onder de Wob. De Wob beschermt belangen van ambtenaren. In een weigeringsgrond, maar ook door ze te betrekken bij het openbaar maken van e-mails die herleidbaar zijn naar hen. Dat kan alleen herleidbaar openbaar worden gemaakt als zij toestemming daarvoor geven. Daarnaast is de beveiliging van overheidsdata is op orde, waardoor de kans op een incident niet verandert.

Samenvattend kan worden gesteld dat het risico voor het opslaan van e-mail, op de voorgestelde werkwijze, ingeschat kan worden als acceptabel voor alle risico's, met extra aandacht voor de volgende 3 risico's, die zich in de gele zone bevinden:
1. Risico op inbreuk op de persoonlijke levenssfeer
2. Risico op beschadiging van reputatie
3. Risico's voor bescherming overige (grond)rechten

Voor alle drie de soorten risico's geldt dezelfde toelichting:
In e-mail wordt, naast strikt zakelijke communicatie, ook allerlei informatie gedeeld dat bij onrechtmatig delen een inbreuk kan maken op de persoonlijke levenssfeer, beschadiging van reputatie kan veroorzaken of de bescherming van overige (grond) rechten in gevaar kan brengen. Dit geldt voor zowel burgers en bedrijven als ook voor rijksmedewerkers zelf. De impact hierop kan ernstige gevolgen hebben voor de betrokkenen. De kans dat dit optreedt is echter onwaarschijnlijk.

D. Beschrijving voorgenomen maatregelen

Hieronder beschrijven wij de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van de betrokkenen aan te pakken.

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

17. Maatregelen

In onderdeel C zijn de risico's als acceptabel omschreven. Een drietal bevindt zich in de gele zone, waardoor ze extra aandacht vragen.

In de risicoafweging is meegenomen dat de huidige technische en juridische maatregelen als afdoende worden beschouwd. Specifiek voor de nieuwe werkwijze rondom toegang tot het e-mailarchief zijn een aantal organisatorische maatregelen beschreven. Ook worden specifieke technische maatregelen, specifiek voor het e-mailarchief, beschreven.

Van onderstaande relevante risico's (1, 7 en 10) kan sprake zijn als de opgeslagen e-mail voor oneigenlijke doelen wordt gebruikt, of wordt geopend door een niet-geoorloofde partij. Dit kan het geval zijn wanneer medewerkers met toegang tot de opgeslagen e-mail (bijvoorbeeld systeembeheerders/administrators van ICT-dienstverleners) deze onrechtmatig delen met derden, deze voor oneigenlijke doeleinden zelf gebruiken of anderszins niet integer behandelen.

Daarnaast is er het risico op toegang tot de opgeslagen e-mail door derden, bijvoorbeeld door hacken of data-lekken. Dit is een algemeen risico dat geldt voor de gehele Rijksoverheid, waar voor de gehele Rijksoverheid afdoende maatregelen zijn genomen.

Onderstaand zijn een drietal categorieën maatregelen beschreven. Door de aard van het onderwerp gelden de maatregelen voor alle benoemde risico's en realiseren ze een verbetering van de kans (kans wordt kleiner) op het optreden van het risico.

Technische maatregelen
Uit het oogpunt van risico's is de toegang/autorisatie tot het gebruik van deze opslag van belang. Daarom worden alleen specifiek geautoriseerde medewerkers met een concrete onderzoeksvraag tijdelijk toegang verleent tot de op deze wijze opgeslagen e-mail. Randvoorwaardelijk daarbij is het doel waarmee eventueel gezocht wordt. Dat moet altijd een informatievraag zijn zonder welke niet kan worden voldaan aan de informatieplicht van bewindspersonen als bedoeld in art. 68 van de grondwet. Deze informatievraag en de daaruit voortvloeiende zoekvragen (queries) worden van tevoren vastgelegd.

In het begin van het proces zijn ook technische maatregelen mogelijk. Te denken valt aan een waarschuwingsfunctie in het e-mailprogramma zelf, waarbij de e-mailberichten worden gemarkeerd (bijv. met een kleurcode) die op korte termijn gaan worden gearchiveerd, tenzij daartegen actie wordt ondernomen.[14]

Organisatorische maatregelen

Het beleid en de procedures rond de uitvoering van informatieverzoeken dienen per ministerie expliciet te worden vastgesteld. Deze afspraken dienen regelmatig te worden geactualiseerd en getoetst aan de AVG.

Het is niet de bedoeling de opslag van de e-mails voor een ander doel dan hiervoor beschreven te gebruiken. Er wordt geen statistische analyse uitgevoerd, geen rangschikking of vorming van een database anders dan de standaard metadata die in elke e-mail aanwezig is (zoals afzender/ontvanger/datum/tijd/onderwerp regel). Het is ook niet het doel om geautomatiseerde besluitvorming, trendanalyse of andere analyses met behulp van algoritmen uit te voeren op de opgeslagen e-mail.

Daarnaast kunnen bewustwordingsprogramma's medewerkers structureel informeren over de gang van zaken. Een belangrijk onderdeel zal zijn dat de medewerker gedurende tien weken in de gelegenheid wordt gesteld om zelf de e-mailberichten te verwijderen die naar zijn oordeel voor de naleving van de wettelijke plicht of de taak van algemeen belang onnodig zijn.[15] Bijvoorbeeld door eens in de zoveel weken een e-mail naar de mailbox te versturen: "denkt u wel aan het schonen van uw mailbox en het verplaatsen van privé e-mails naar de map privé?"

Juridische maatregelen

Voor alle medewerkers van alle betrokken instanties geldt een algemene geheimhoudingsplicht met betrekking tot de verwerkte gegevens. De geheimhoudingsplicht voor Rijksmedewerkers geldt uit hoofde van artikel 125a, derde lid, van de Ambtenarenwet. Er is geen sprake van een geheimhoudingsplicht die in de weg staat aan de onderhavige verwerking van persoonsgegevens. Deze geheimhoudingsplicht vermindert het risico op ondoelmatig gebruik en verspreiden van onderzoekdata.

Informatie uit e-mails die relevant is in de beantwoording op informatieverzoeken als bedoeld in art. 68 grondwet kan (deels) openbaar worden gemaakt. Daarbij worden, conform het daarvoor gestelde eisen in de Wob, persoonsgegevens onherkenbaar gemaakt om de privacy van betrokkenen te beschermen.

Bewustwording en transparantie worden verbeterd door ook de anderen, over wie persoonsgegevens zijn opgenomen in het desbetreffende e-mailbericht, te informeren. Voor de hand ligt om ten minste in ieder e-mailbericht tekst daartoe op te nemen, wellicht met daarbij een verwijzing (link) naar een uitgebreidere privacyverklaring waarin alle in relevante informatie (zie art. 12 t/m 14 AVG) wordt gegeven. Ook kan wellicht, waar e-mailadressen van rijksambtenaren bekend worden gemaakt, worden aangegeven dat op de daar naartoe verstuurde berichten het zgn. «emailbewaarbeleid van de Rijksoverheid» van toepassing is. Ten slotte ligt voor de hand om bij de rijksambtenaren onder de aandacht te brengen dat het, om deze redenen, wordt afgeraden om privé-berichten vanuit werkaccounts te versturen.[16]

[14] Citaat uit advies 'Advocaten Brinkhof' (13 mei 2018)
[15] Citaat uit advies 'Advocaten Brinkhof' (13 mei 2018)
[16] Citaat uit advies 'Advocaten Brinkhof' (13 mei 2018)

Bepaling risico na extra maatregelen

Met het in acht nemen van de extra maatregelen schatten wij de risico's als volgt in:

nr.	Risico	Impact	Kans	Risicozone
1.	Risico op inbreuk op de persoonlijke levenssfeer	Ernstig	Zeer onwaarschijnlijk	Groen
2.	Risico op aanzienlijk economisch of maatschappelijk nadeel	Matig	Zeer onwaarschijnlijk	Groen
3.	Risico op inbreuk op de bescherming van de lichamelijke integriteit	Klein	Zeer onwaarschijnlijk	Groen
4.	Risico op onrechtvaardige behandeling	Matig	Zeer onwaarschijnlijk	Groen
5.	Risico op ongelijke behandeling	Matig	Zeer onwaarschijnlijk	Groen
6.	Risico op aantasting van de autonomie	Matig	Zeer onwaarschijnlijk	Groen
7.	Risico op beschadiging van reputatie	Ernstig	Zeer onwaarschijnlijk	Groen
8.	Risico's voor de veiligheid van de respondent en/of zijn familie	Matig	Zeer onwaarschijnlijk	Groen
9.	Risico op aantasting menselijke waardigheid	Matig	Zeer onwaarschijnlijk	Groen
10.	Risico's voor bescherming overige (grond)rechten	Ernstig	Zeer onwaarschijnlijk	Groen

Samenvattend kan worden gesteld dat het risico voor het opslaan van e-mail, op de voorgestelde werkwijze, ingeschat kan worden als acceptabel voor alle risico's. Alle risico's bevinden zich in de groene zone.

Dit is een uitgave van:

Rijksprogramma Duurzaam Digitale
Informatiehuishouding (RDDI)

23 mei 2018