SSC-ICT
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Onderzoek naar de technische mogelijkheden van implementatie van de *Handreiking bewaren van e-mail Rijksoverheid* met standaardfunctionaliteiten binnen Microsoft Exchange

Tussenrapport fase 1a

Versie	1.0
Datum	1 april 2020
Status	Definitief

Colofon

Titel	Onderzoek naar de technische mogelijkheden van implementatie van de *Handreiking bewaren van e-mail Rijksoverheid* met standaard-functionaliteiten binnen Microsoft Exchange. Tussenrapport fase 1a
Opdrachtgever	Rijksprogramma voor Duurzaam Digitale Informatiehuishouding (RDDI) Project E-mailarchivering
Afzendergegevens	SSC-ICT Koningskade 4 2596 AA Den Haag 088 371 0100 www.ssc-ict.nl
Versienummer	1.0 | Definitief | Geanonimiseerd
Auteur	(geanonimiseerd)
Auteur	(geanonimiseerd)
Relatiemanager	(geanonimiseerd)
	Met eventuele vragen kunt u contact opnemen met RDDI via informatiehuishouding@minocw.nl.

Inhoud

Managementsamenvatting

Aanleiding en opdracht
In de *Handreiking Bewaren van e-mail Rijksoverheid* (hierna: *Handreiking*) staat de werkwijze voor het bewaren van e-mail beschreven. Het Rijks-programma voor Duurzaam Digitale Informatiehuishouding (hierna: RDDI) heeft SSC-ICT opdracht gegeven een onderzoek uit te voeren naar de mogelijkheden om de werkwijze uit de *Handreiking* technisch te implementeren *binnen* een Microsoft Exchange-omgeving. Het onderzoek heeft betrekking op een Microsoft Exchange-omgeving *in het algemeen*, en niet op een bestaande Exchange-omgeving zoals die is ingericht bij SSC-ICT of elders binnen de Rijksoverheid. De opdracht betreft ook niet het identificeren van oplossingen *buiten* Microsoft Exchange.

De opdracht voor het onderzoek vloeit voort uit de wens om bij de toepassing van de *Handreiking* zoveel mogelijk uit te gaan van geautomatiseerde oplossingen, om op die manier de medewerkers binnen de Rijksoverheid maximaal te ontzorgen. Daar waar een geautomatiseerde oplossing voorhanden is, zijn immers veel minder tot geen organisatorische oplossingen nodig.

Deze geautomatiseerde oplossingen zijn in dit onderzoek gezocht binnen de Microsoft Exchange-omgeving en toegespitst op generieke standaardoplossingen, omdat die ten dienste kunnen staan van alle (rijks)organisaties die de *Handreiking* willen implementeren. Deze afbakening ondersteunt de toekomstvastheid en de beheerbaarheid van de oplossing. Standaardfunctionaliteiten zullen namelijk in toekomstige softwareversies vrijwel zeker blijven bestaan, terwijl het onzeker is of zelf geprogrammeerde maatwerkoplossingen dan blijven functioneren. Overigens wordt de huidige versie van Exchange Server tot eind 2025 ondersteund door Microsoft. Dat betekent dat voor die tijd de software(versie) al zal wijzigen. Mogelijk biedt Microsoft na die tijd alleen nog de Cloud-versie Exchange Online aan.

Reikwijdte en aanpak van het onderzoek
Het onderzoek is opgedeeld in fase 1a en 1b. Dit is het tussenrapport ter afronding van fase 1a. Aan het begin van fase 1a heeft de opdrachtgever onder penvoering van SSC-ICT eerst een nadere interpretatie van een deel van de uitgangspunten van de *Handreiking* naar technische eisen en wensen opgesteld. In deze fase is dat beperkt tot drie van de vier hoofd-functionaliteiten die in de *Handreiking* staan (*Veiligstellen*, *Uitzonderen van veiligstellen* en *Vernietigen*); de vierde (*Overdragen*) zal in fase 1b worden geïnterpreteerd. Het resultaat is vastgelegd in de *Interpretatie van de Handreiking bewaren e-mail Rijksoverheid* (hierna: *Interpretatie*).

Uit de *Interpretatie* zijn daarna door SSC-ICT eenentwintig eisen aan de technische oplossing geïdentificeerd. SSC-ICT heeft, na overleg met Microsoft, voor elk van deze eenentwintig eisen ingeschat of de kans klein, middel of groot is dat ofwel (a) de eis technisch onuitvoerbaar is, ofwel (b) dat aan de oplossing grote risico's of nadelen kleven. De opdrachtgever heeft, om de doorlooptijd van fase 1a te bekorten, vervolgens het

onderzoek in fase 1a beperkt tot de negen eisen met een grote kans. Die negen eisen zijn kort beschreven in de navolgende tabel.

Voor elk van de negen onderzochte eisen wordt in dit tussenrapport het volgende beschreven:
- wat de eis inhoudt;
- of de eis technisch mogelijk is met standaardfunctionaliteiten van Microsoft Exchange (zo ja, hoe; zo nee, waarom niet);
- wat de nadelen en risico's zijn van de oplossing voor die eis.

De negen onderzochte eisen zijn getoetst aan de technische uitvoerbaarheid met de standaardfunctionaliteiten van Microsoft Exchange. Daarbij is niet alleen uitgegaan van de kennis en expertise van de specialisten, architecten en adviseurs van SSC-ICT, maar is ook gedetailleerd overlegd met drie experts van Microsoft over de mogelijkheden van Microsoft Exchange. De technische toetsing in dit tussenrapport is ook gereviewd door Microsoft.

Op basis van de resultaten van dit tussenrapport zal de opdrachtgever (RDDI) besluiten over het al dan niet uitvoering geven aan fase 1b en – bij een 'go' – over eventuele aanpassing van de opdracht. Fase 1b zal in principe de twaalf eisen omvatten die wel zijn geïdentificeerd in fase 1a, maar nog niet zijn onderzocht, en daarnaast ook de eisen die nog voortvloeien uit het deel van de *Handreiking* dat nog niet is geïnterpreteerd. In fase 1b zullen ook andere aspecten worden onderzocht, zoals een globale inschatting van de kosten en de termijn waarop de oplossing kan worden gerealiseerd.

Onderzoeksresultaten
De uitkomsten zijn samengevat weergegeven in de tabel op de volgende pagina. Daarin staat achtereenvolgens weergegeven: een korte samenvatting van de eis, of een technische oplossing mogelijk is met de standaardfunctionaliteiten van Microsoft Exchange, en of er nadelen en risico's aan de oplossing kleven. Daarbij is eis 8 opgesplitst in 8a en 8b. Alleen als een oplossing helemaal voldoet aan een eis, wordt deze met een vink aangegeven. De oplossing bij eis 2 en 3 voldoet slechts gedeeltelijk aan de eis en is daarom met een oranje kruis weergegeven.

Voor zover een oplossing (deels) mogelijk is, betreffen de geïdentificeerde risico's daarvan onder meer:
- De stabiliteit van de e-mailomgeving kan niet worden gegarandeerd;
- Voor veel eindgebruikers kan het regulier werken met e-mail worden verhinderd, als gevolg van oplopende vertragingen in het lezen, verzenden en ontvangen van e-mail;
- Er is een verhoogde kans op verstoringen die ook nog eens lastiger zijn te verhelpen, temeer omdat Microsoft geen enkele klant kent die een soortgelijke oplossing heeft geïmplementeerd;
- Performancetesten geven zelfs geen zekerheid van stabiliteit op de lange termijn;
- Vooraf kunnen de financiële gevolgen van een implementatie niet worden ingeschat, doordat van tevoren niet kan worden bepaald hoeveel extra hardware en beheerinspanning benodigd is;

- De implementatie (voor zover mogelijk) is zo gecompliceerd, dat de werking en werkwijze niet eenvoudig kan worden uitgelegd aan de eindgebruikers.

Eis	Technische oplossing in Microsoft Exchange	Nadelen en risico's
Eis 1: E-mail wordt tien weken na ontvangst/verzending veiliggesteld	✔ Mogelijk	✘ Serieuze nadelen en risico's
Eis 2: Veiliggestelde e-mails na tien jaar vernietigen	✘ Slechts deels mogelijk	✘ Serieuze nadelen en risico's
Eis 3: Eindgebruiker kan e-mail vernietigen binnen tien weken na ontvangst/verzending	✘ Slechts deels mogelijk	✘ Serieuze nadelen en risico's
Eis 4: Terughalen verwijderde e-mail binnen tienwekentermijn	✘ Geheel niet mogelijk	
Eis 5: Terughalen verwijderde e-mail nog korte tijd na tienwekentermijn mogelijk	✘ Geheel niet mogelijk	
Eis 6: Eindgebruiker kan e-mail binnen tien weken na ontvangst/verzending aanmerken als privé	✔ Mogelijk	
Eis 7: Eindgebruiker kan na tien weken e-mail niet meer als privé aanmerken	✘ Geheel niet mogelijk	
Eis 8a: Zorgdrager kan na tien weken e-mail nog wel vernietigen	✘ Geheel niet mogelijk	
Eis 8b: Zorgdrager kan na tien weken e-mail nog wel als privé aanmerken	✔ Mogelijk	✘ Serieuze nadelen
Eis 9: Als privé aangemerkte e-mails worden niet na tien jaar automatisch vernietigd	✔ Mogelijk	✘ Serieuze nadelen en risico's

Conclusie
Uit het onderzoek blijkt dat de werkwijze uit de *Handreiking* niet kan worden geïmplementeerd met de standaardfunctionaliteiten binnen Microsoft Exchange. Voor het merendeel van de onderzochte negen eisen blijkt namelijk geen technische oplossing binnen de standaard-functionaliteiten binnen Microsoft Exchange te bestaan. Voor enkele eisen bestaat wel een technische oplossing, maar die oplossingen gaan echter gepaard met serieuze nadelen en risico's voor onder meer de stabiliteit en betrouwbaarheid van de e-maildienstverlening aan de eindgebruikers. Deze conclusie zal overigens ook niet wijzigen als uit fase 1b eventueel zou blijken dat voor alle overige eisen een technische oplossing wel volledig mogelijk zou zijn zonder nadelen of risico's.

1. Inleiding

In de *Handreiking Bewaren van e-mail Rijksoverheid* (hierna: *Handreiking*[1]) staat de werkwijze voor het bewaren van e-mail beschreven. Het Rijksprogramma voor Duurzaam Digitale Informatiehuishouding (hierna: RDDI) heeft SSC-ICT opdracht gegeven een onderzoek uit te voeren naar de mogelijkheden om de werkwijze uit de *Handreiking* technisch te implementeren *binnen* een Microsoft Exchange-omgeving. Microsoft Exchange is namelijk het softwareplatform dat door vrijwel de gehele overheid wordt gebruikt voor de mailvoorziening.[2] Het onderzoek heeft betrekking op een Microsoft Exchange-omgeving *in het algemeen*, en niet op een bestaande Exchange-omgeving zoals die is ingericht binnen SSC-ICT of elders binnen de Rijksoverheid.

De opdracht voor het onderzoek vloeit voort uit de wens om bij de toepassing van de *Handreiking* zoveel mogelijk uit te gaan van geautomatiseerde oplossingen, om op die manier de medewerkers binnen de Rijksoverheid maximaal te ontzorgen. Daar waar een geautomatiseerde oplossing voorhanden is, zijn immers veel minder tot geen organisatorische oplossingen nodig.

Deze geautomatiseerde oplossingen zijn in dit onderzoek gezocht binnen de Microsoft Exchange-omgeving en toegespitst op generieke standaardoplossingen. De opdrachtgever streeft naar (geautomatiseerde) generieke standaardoplossingen, omdat die ten dienste kunnen staan van alle (rijks)organisaties die de *Handreiking* willen implementeren. Om die reden gaat de voorkeur van de opdrachtgever vooralsnog niet uit naar maatwerkoplossingen en/of alternatieve (*third party*) oplossingen. Deze afbakening ondersteunt de toekomstvastheid en de beheerbaarheid van de oplossing. Standaardfunctionaliteiten zullen namelijk in toekomstige softwareversies vrijwel zeker blijven bestaan, terwijl het onzeker is of zelf geprogrammeerde maatwerkoplossingen dan blijven functioneren. Overigens wordt de huidige versie van Exchange Server tot eind 2025 ondersteund door Microsoft. Dat betekent dat voor die tijd de software(versie) al zal wijzigen. Mogelijk biedt Microsoft na die tijd alleen nog de Cloud-versie Exchange Online aan.

[1] Zie bijlage 1 en tevens https://www.informatiehuishouding.nl/
[2] Zo levert SSC-ICT bijvoorbeeld aan de zeven ministeries die zij als klant heeft de mailvoorziening op basis van Microsoft Exchange. Die mailomgeving is via de mobiele werkomgeving (smartphone en tablet) toegankelijk via een BlackBerry-applicatie. In dit onderzoek is echter gekeken naar een algemene Exchange-installatie, niet naar de huidige mailomgeving van SSC-ICT. SSC-ICT voert dit onderzoek uit omdat zij, als leverancier aan zeven ministeries, bekend is met de rijksbrede context en met het leveren van e-maildienstverlening op basis van Microsoft Exchange.

Het onderzoek is opgedeeld in fase 1a en fase 1b. In fase 1a zijn negen van de eenentwintig geïdentificeerde eisen onderzocht op technische haalbaarheid. Fase 1a is met dit tussenrapport afgerond. Op basis van de resultaten van dit tussenrapport zal de opdrachtgever (RDDI) besluiten over het al dan niet uitvoering geven aan fase 1b en – bij een 'go' – over eventuele aanpassing van de opdracht.

Bij dit onderzoek is RDDI de opdrachtgever en SSC-ICT de opdrachtnemer. SSC-ICT heeft daarbij Microsoft als leverancier van Exchange betrokken; experts van Microsoft zijn inhoudelijk geraadpleegd en hebben de technische toetsing in dit tussenrapport gereviewd. Het onderzoek is vanuit de opdrachtgever begeleid door een begeleidingsgroep, die met SSC-ICT als penvoerder ook de *Handreiking* heeft geïnterpreteerd naar concrete eisen en wensen.[3]

Dit tussenrapport is als volgt opgebouwd. In hoofdstuk 2 staan de onderzoeksopdracht en de afbakening van fase 1a ten opzichte van fase 1b. In hoofdstuk 3 staan vervolgens de negen onderzochte eisen weergegeven. Hoofdstuk 4 beschrijft de functionaliteiten van Microsoft Exchange die bij het onderzoek zijn betrokken, waarna in hoofdstuk 5 per onderzochte eis de technische oplossingen staan. Ten slotte bevat hoofdstuk 6 de conclusie van het onderzoek.

[3] De deelnemers van de begeleidingsgroep en de betrokkenen vanuit SSC-ICT en Microsoft staan in bijlage 4.

2. Onderzoeksopdracht en -aanpak

2.1. Onderzoeksopdracht

RDDI heeft SSC-ICT opdracht gegeven voor een onderzoek naar de technische oplossingsrichtingen voor de implementatie van de *Handreiking* technisch te implementeren *binnen* een Microsoft Exchange-omgeving, zonder gebruik te maken van andere hard- en software. Het onderzoek richt zich op het gebruik van standaardfunctionaliteiten van Microsoft Exchange. Die standaardfunctionaliteiten zullen in toekomstige softwareversies vrijwel zeker blijven bestaan, terwijl het onzeker is of zelf geprogrammeerde maatwerkoplossingen dan blijven functioneren. Dat draagt eraan bij dat de implementatie toekomstvast en beheerbaar blijft. Bij het technische onderzoek naar de oplossingen zijn ook specialisten van Microsoft betrokken.

De onderzoeksopdracht bevat een splitsing van het onderzoek in twee fasen (1a en 1b). Dit is het tussenrapport waarmee fase 1a wordt afgerond.

2.2. Reikwijdte onderzoek fase 1a

In fase 1a is eerst een nadere interpretatie van een deel van de uitgangspunten van de Handreiking naar technische eisen en wensen vastgesteld. In deze fase is dat beperkt tot drie van de vier hoofdfunctionaliteiten die in de *Handreiking* staan (*Veiligstellen*, *Uitzonderen van veiligstellen* en *Vernietigen*); de vierde (*Overdragen*) wordt in fase 1b geïnterpreteerd.[4] De uitkomsten van de interpretatie en de initiële afbakening van fase 1a zijn vastgelegd in de *Interpretatie van de Handreiking bewaren e-mail Rijksoverheid* (hierna: *Interpretatie*). De *Interpretatie* is integraal opgenomen als bijlage 2.

Uit de *Interpretatie* zijn door SSC-ICT eenentwintig eisen en wensen geïdentificeerd. SSC-ICT heeft voor elk van de eenentwintig eisen ingeschat of de kans klein, middel of groot is dat ofwel de eis technisch onuitvoerbaar is, ofwel dat aan de oplossing grote risico's of nadelen kleven, zie bijlage 3. Die inschatting is gemaakt op basis van de voorlopige inzichten bij SSC-ICT die mede door de gesprekken met de experts van Microsoft zijn ontstaan. De opdrachtgever heeft, om de doorlooptijd van fase 1a te bekorten, vervolgens het onderzoek in fase 1a beperkt tot de negen eisen met een grote kans daarop.[5] Daarmee zijn de meest kritieke eisen onderzocht. De negen onderzochte eisen staan in hoofdstuk 3 beschreven.

[4] Zie verder paragraaf 3.1.
[5] De uiteindelijke reikwijdte van fase 1a is daarmee kleiner dan de aanvankelijke opdracht. Dat verklaart dat in de *Interpretatie* (opgenomen als bijlage 2) nog een ruimere scope voor fase 1a is beschreven.

Voor elk van de negen onderzochte eisen wordt in dit tussenrapport van fase 1a het volgende beschreven:
- wat de eis inhoudt;
- of de eis technisch mogelijk is met standaardfunctionaliteiten van Microsoft Exchange (zo ja, hoe; zo nee, waarom niet);
- wat de nadelen en risico's zijn van de oplossing voor die eis.

Fase 1b omvat de twaalf eisen die wel zijn geïdentificeerd, maar niet in fase 1a worden onderzocht, en daarnaast ook de eisen die nog voortvloeien uit het deel van de *Handreiking* dat nog niet is geïnterpreteerd. In fase 1b worden ook andere aspecten van deze oplossingsrichtingen onderzocht, zoals een globale inschatting van de kosten en de termijn waarop de oplossing kan worden gerealiseerd.

2.3. Reikwijdte onderzoek fase 1b

In fase 1b zal een volledige implementatie van de *Handreiking* worden onderzocht. Voor elk van de oplossingsrichtingen wordt dan het volgende beschreven: een beschrijving van de oplossingsrichting (zonder een technisch ontwerp), de functionaliteit daarvan en (voor zover bekend) de voor- en nadelen vanuit het perspectief van gebruikers, departementen en de beheerorganisatie; de termijn waarop de oplossing kan worden gerealiseerd; een globale inschatting van de kosten en de geïdentificeerde aandachtspunten, risico's en de mate waarin de oplossing voldoet aan de *Handreiking*. Ook omvat fase 1b een suggestie vanuit SSC-ICT voor een voorkeursoplossing vanuit het perspectief van techniek, het beheer van de omgeving en de toekomstvastheid (technische duurzaamheid). Tevens omvat fase 1b enkele aanvullende eisen in het kader van duurzame toegankelijkheid en een onderzoek naar de mogelijkheden om de e-mail te doorzoeken (Zoek-en-Vind). Dat levert een eindrapport op.

Overigens kan de reikwijdte voor fase 1b nog wijzigen. Na fase 1a zal de opdrachtgever (RDDI) namelijk besluiten over het al dan niet uitvoering geven aan fase 1b en – bij een 'go' – over eventuele aanpassing van de opdracht.

2.4. Oplossingsrichtingen buiten scope

De onderzoeksopdracht is (voor beide fasen) steeds beperkt geweest tot een implementatie binnen de Microsoft Exchange-omgeving. Voor de volledigheid wordt daarom opgemerkt dat oplossingen waarbij de e-mailgegevens *buiten* de Exchange-omgeving worden opgeslagen, expliciet *niet* in de scope van het onderzoek zitten.[6] Het onderzoek richt zich op het gebruik van standaardfunctionaliteiten van Microsoft Exchange. Die standaardfunctionaliteiten zullen in toekomstige softwareversies vrijwel zeker blijven bestaan, terwijl het

[6] Buiten de scope van dit onderzoek valt dus bijvoorbeeld een oplossingsrichting waarbij via *journaling* een kopie van alle e-mails in een afzonderlijk systeem wordt bewaard. Eveneens buiten scope valt onder andere een oplossingsrichting, waarbij een kopie van gegevens uit de Exchange-omgeving in een afzonderlijk systeem wordt bewaard.

onzeker is of zelf geprogrammeerde maatwerkoplossingen dan blijven functioneren. Dat draagt eraan bij dat de implementatie toekomstvast en beheerbaar blijft. Een migratie naar een andere versie is vóór oktober 2025 voorzien, omdat op dat moment de ondersteuning van Microsoft voor de huidige versie van Exchange Server zal eindigen. Mogelijk biedt Microsoft na die tijd alleen de Cloud-versie Exchange Online aan.

2.5. Onderzoeksaanpak fase 1a

Het onderzoek (fase 1a) is opgedeeld in twee delen: een interpretatiefase en een onderzoeksfase.

2.5.1. Interpretatiefase

In de *Handreiking* staat de werkwijze voor het bewaren van e-mail beschreven. Aangezien de *Handreiking* niet het karakter heeft van een functioneel ontwerp, was een nadere interpretatie van de uitgangspunten van een deel van de Handreiking naar technische eisen en wensen nodig om het onderzoek uit te kunnen voeren. Deze fase had tot doel om die nadere interpretatie uit te voeren. In fase 1a is dat beperkt tot drie van de vier hoofdfunctionaliteiten die in de *Handreiking* staan (*Veiligstellen*, *Uitzonderen van veiligstellen* en *Vernietigen*); de vierde (*Overdragen*) wordt in fase 1b geïnterpreteerd.[7]

In interne overleggen hebben diverse specialisten van SSC-ICT de *Handreiking* doorgenomen en zijn vragen en opmerkingen geïdentificeerd. Die vragen zijn in enkele overleggen samen met een begeleidingsgroep[8] van RDDI doorgenomen en van antwoorden voorzien. Die vragen en antwoorden zijn verwerkt in een conceptversie van de *Interpretatie*. Dat concept is in meerdere iteraties besproken met de begeleidingsgroep, waarbij veel aandacht is geschonken aan een zorgvuldige formulering. Ook is daarbij in de *Interpretatie* duidelijk aangegeven welke eisen en wensen in fase 1a worden onderzocht.[9] Deze werkwijze, waarbij SSC-ICT de rol van facilitator en penvoerder had, heeft geresulteerd in de vaststelling van de vastgestelde definitieve versie van de *Interpretatie* door de opdrachtgever.

2.5.2. Onderzoeksfase

In de onderzoeksfase heeft SSC-ICT uit de *Interpretatie* de eenentwintig afzonderlijke eisen en wensen voor fase 1a afgeleid. Vervolgens hebben de specialisten van SSC-ICT met de experts van Microsoft de standaardfunctionaliteiten van Microsoft Exchange gedetailleerd besproken, met het oog op de mogelijkheden om de eenentwintig eisen daarmee te kunnen implementeren. Met die kennis heeft SSC-ICT per eis een inschatting gemaakt van de kans dat ofwel de eis technisch onuitvoerbaar is, ofwel dat aan de oplossing grote

[7] Zie verder paragraaf 3.1.
[8] In bijlage 4 zijn de deelnemers aan de begeleidingsgroep vermeld.
[9] De opdrachtgever heeft op een later moment de reikwijdte van fase 1a beperkt tot de negen onderzochte eisen.

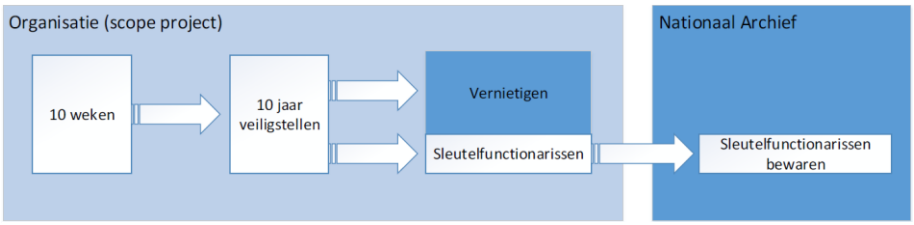
risico's of nadelen kleven.[10] Daarna heeft de opdrachtgever de scope omwille van de doorlooptijd beperkt tot de negen eisen waarvoor die kans groot is. Voor die negen eisen zijn de antwoorden op de onderzoeksvragen (zie paragraaf 2.2) opgesteld. Daarbij is niet alleen uitgegaan van de kennis en expertise van de specialisten van SSC-ICT,[11] maar is ook gedetailleerd overlegd met experts van Microsoft over de mogelijkheden van Microsoft Exchange.

[10] In bijlage 3 staan de eenentwintig eisen, met daarbij ook de geschatte kans.
[11] Naast Exchange-specialisten zijn ook domeinarchitecten en security- en privacy-adviseurs van SSC-ICT bij het onderzoek betrokken.

3. De negen onderzochte eisen

3.1. Werkwijze op hoofdlijnen

De werkwijze die in de *Handreiking* staat beschreven, kan worden opgedeeld in vier hoofdfunctionaliteiten:
(1) het **Veiligstellen** van alle e-mails voor een periode van tien jaar;
(2) het **Uitzonderen** van veiligstellen van specifieke e-mails in de eerste tien weken;
(3) het **Vernietigen** van de veiliggestelde e-mails na tien jaar, en
(4) het **Overdragen** van een deel van de e-mails aan het Nationaal Archief na tien jaar.



Figuur 1. Werkwijze E-mail bewaren. (Bron: *Handreiking Bewaren van E-mail Rijksoverheid*)

Voor de drie hoofdfunctionaliteiten *Veiligstellen*, *Uitzonderen van veiligstellen* en *Vernietigen* is een nadere interpretatie van de uitgangspunten van de Handreiking naar eisen en wensen opgesteld. Dat is de eerdergenoemde *Interpretatie*. Voor de vierde hoofdfunctionaliteit *Overdragen* zal die interpretatie tijdens fase 1b plaatsvinden, aangezien de hoofdfunctionaliteit *Overdragen* in zijn geheel in fase 1b zal worden onderzocht. De eisen en wensen die voor de eerste drie hoofd-functionaliteiten in de *Interpretatie* zijn geïdentificeerd, staan opgesomd in bijlage 3.

In de *Interpretatie* staat ook een uitgebreid begrippenkader (zie bijlage 2). De begrippen in dit tussenrapport hebben dezelfde betekenis als in dat begrippenkader.

3.2. Negen onderzochte eisen

Op basis van de voorlopige inzichten bij SSC-ICT door de gesprekken met de experts van Microsoft, heeft SSC-ICT ingeschat dat negen eisen een grote kans hebben dat ofwel de eis technisch onuitvoerbaar is, ofwel dat aan de oplossing grote risico's of nadelen kleven. Deze negen eisen worden hieronder opgesomd, waarbij de toelichting woordelijk is overgenomen uit de *Interpretatie*. Daarbij is steeds vermeld in welke paragraaf van de *Interpretatie* de eis is beschreven. Deze negen onderzochte eisen zijn dus maar een deel van de eisen die voortvloeien uit de *Handreiking* en de *Interpretatie*.

3.2.1. Eis 1: E-mail wordt tien weken na ontvangst/verzending veiliggesteld

E-mail wordt tien weken na ontvangst/verzending veiliggesteld.[12] In de praktijk is het misschien technisch niet mogelijk om dit op de seconde nauwkeurig tien weken na ontvangst/verzending van de e-mail te doen. Het veiligstellen mag dan ook batchgewijs zo snel mogelijk na afloop van de tienwekentermijn.[13] (Zie paragraaf 4.2 van de *Interpretatie*.)

3.2.2. Eis 2: Veiliggestelde e-mails na tien jaar vernietigen

E-mail die is veiliggesteld, wordt op een zeker moment vernietigd. Voor alle veiliggestelde e-mails zal die vernietiging plaatsvinden tien jaar na ontvangst/verzending van de e-mail. Het moment van vernietigen ligt niet per definitie direct/exact na afloop van de bewaartermijn van tien jaar. Het vernietigen zelf kost immers ook tijd. Het heeft de voorkeur dat de vernietiging niet te lang na afloop van de tienjaarstermijn plaatsvindt. Dat kan bijvoorbeeld in maandelijkse batches. (Zie paragraaf 6.1 en 6.3 van de *Interpretatie*.)

3.2.3. Eis 3: Eindgebruiker kan e-mail vernietigen binnen tien weken na ontvangst/verzending

In de eerste tien weken na ontvangst/verzending van de e-mail, kan de eindgebruiker de e-mail verwijderen. De verwijderde e-mail is daarna nog enige tijd terug te halen, voor het geval de eindgebruiker de e-mail abusievelijk heeft verwijderd. Daarna wordt de e-mail technisch vernietigd, wat betekent dat de inhoud van de e-mail niet meer kan worden gereconstrueerd. (Zie paragraaf 5.2 van de *Interpretatie*.)

3.2.4. Eis 4: Terughalen verwijderde e-mail binnen tienwekentermijn

Binnen de tienwekentermijn moet een (abusievelijk) verwijderde e-mail nog kunnen worden teruggehaald, zodat de verwijdering ongedaan gemaakt wordt. De verwijderde e-mail mag dus pas na afloop van de tienwekentermijn technisch worden vernietigd. (Zie paragraaf 5.2 van de *Interpretatie*.)

3.2.5. Eis 5: Terughalen verwijderde e-mail nog korte tijd na tienwekentermijn mogelijk

Die technische vernietiging mag onmiddellijk na afloop van die tienwekentermijn plaatsvinden. Het heeft echter de voorkeur als een verwijderd bericht ook na de tienwekentermijn nog een korte tijd behouden blijft, en pas na die korte tijd technisch wordt vernietigd. Dan is het namelijk mogelijk om binnen die korte tijd na afloop van de tienwekentermijn een (abusievelijk) verwijderde e-mail nog terug te halen. Die korte tijd kan nader worden bepaald en ligt in de orde van grootte van een paar weken, zodat die korte tijd in verhouding staat

[12] Het veiligstellen van een e-mail betekent dat gedurende een vastgestelde periode de oorspronkelijke e-mail niet kan worden vernietigd.
[13] De tienwekentermijn betreft de eerste tien weken na het moment van ontvangst/verzending van een e-mail. Elke e-mail heeft een eigen tienwekentermijn.

tot de tienwekentermijn. (Zie paragraaf 5.2 van de *Interpretatie*.)

3.2.6. *Eis 6: Eindgebruiker kan e-mail binnen tien weken na ontvangst/verzending aanmerken als privé*
Een eindgebruiker kan een e-mail binnen tien weken na ontvangst/verzending aanmerken als privé. Deze functionaliteit is bedoeld om het mogelijk te maken dat niet-relevante e-mail wordt uitgezonderd van veiligstellen. (Zie paragraaf 5.3 van de *Interpretatie*.)

3.2.7. *Eis 7: Eindgebruiker kan na tien weken e-mail niet meer als privé aanmerken*
Het moet onmogelijk zijn voor de eindgebruiker zelf om een veiliggestelde e-mail na de tienwekentermijn alsnog als privé aan te merken. (Zie paragraaf 4.4 van de *Interpretatie*.)

3.2.8. *Eis 8: Zorgdrager kan na tien weken e-mail nog wel vernietigen of als privé aanmerken*
Het moet echter wel mogelijk zijn dat de zorgdrager aan de ICT-leverancier een opdracht geeft om een veiliggestelde e-mail na de tienwekentermijn alsnog te vernietigen, of als privé aan te merken. (Zie paragraaf 4.4 van de *Interpretatie*.)

3.2.9. *Eis 9: Als privé aangemerkte e-mails worden niet na tien jaar automatisch vernietigd*
E-mails die zijn uitgezonderd van veiligstellen door ze als privé aan te merken, worden niet vernietigd, omdat ze niet zijn veiliggesteld. (Zie paragraaf 6.2 van de *Interpretatie*.)

4. Functionaliteiten in Exchange

4.1. Inleiding

Microsoft Exchange biedt standaard een aantal functionaliteiten voor de omgang met e-mailberichten. Sommige functionaliteiten zijn gericht op het borgen van compliance of het genereren van audit trails, met het doel ervoor te zorgen dat alle e-mailuitwisselingen van één of meer mailboxen altijd kunnen worden gereconstrueerd. De e-mails worden dan verwerkt aan de hand van de ouderdom van het bericht. Een deel van de functionaliteiten maakt het mogelijk per ongeluk verwijderde e-mails terug te halen.

Het is nuttig om in dit hoofdstuk eerst de relevante functionaliteiten van Microsoft Exchange weer te geven. Dat dient als referentie bij het lezen van de technische oplossingen en de bijbehorende nadelen en risico's die in het volgende hoofdstuk per eis staan beschreven. In dit hoofdstuk wordt steeds onderscheid gemaakt tussen de functionele werking (wat doet het?) en de techniek daarachter (hoe werkt het?). De lezer kan ervoor kiezen de technische paragrafen over te slaan, en (eerst) alleen de functionele werking te lezen. In paragraaf 4.2 wordt eerst de standaardwerking beschreven en worden enkele begrippen geïntroduceerd. In de daaropvolgende paragrafen wordt zowel functioneel als technisch beschreven hoe de functionaliteiten van die standaardwerking verschillen.

In dit hoofdstuk wordt de **algemene werking** van (de functionaliteiten van) een Exchange-omgeving beschreven. Dit hoofdstuk betreft dus **niet** (een implementatie van) de werkwijze uit de *Handreiking*. Ook bevat dit hoofdstuk uitdrukkelijk **niet** een beschrijving van de huidige inrichting van Exchange bij SSC-ICT.

Overigens bevat dit hoofdstuk volledigheidshalve ook functionaliteiten (zoals *journaling* en de *archive mailbox*) die wel in beeld zijn gekomen bij het onderzoek, maar géén technische oplossing voor de eisen zijn. Paragraaf 4.7 en 4.8 bevatten ook een korte toelichting waarom *journaling* en *archive mailbox* daarvoor geen oplossing zijn. Daarom komen niet alle in dit hoofdstuk belichte functionaliteiten terug bij de oplossingen in hoofdstuk 5.

4.2. Algemene werking Exchange-omgeving

4.2.1. De Recoverable items

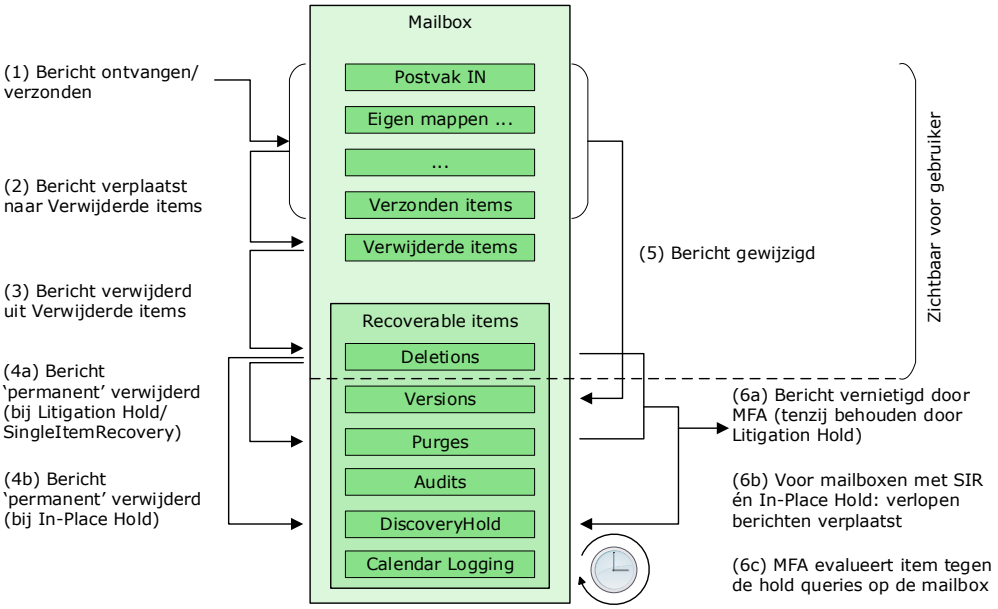
De Exchange-omgeving is de zogenoemde *back-end*, ofwel de servers waarop de e-mails staan. Die omgeving is toegankelijk via Outlook (op de gewone digitale

werkomgeving) of via een mobiele applicatie op de tablet of smartphone.[14]
Elke mailbox bestaat uit twee delen. Een deel is (via Outlook of een mobiele applicatie) zichtbaar voor de eindgebruikers en omvat de standaard zichtbare mappen zoals *Postvak IN*, zelfgemaakte mappen, *Verzonden items*, en *Verwijderde items*. Het andere deel heet *Recoverable items* en bevat een aantal mappen dat onder andere wordt gebruikt voor de speciale functionaliteiten die in dit hoofdstuk worden beschreven. De *Recoverable items* zijn (op de map *Deletions* na, zie verderop) niet zichtbaar voor de eindgebruiker, maar "onder water" wel voor de technisch beheerder.

Voor de beschrijving van de standaardwerking wordt Figuur 2 in paragraaf 4.2.2 gebruikt. Daarin staan ook al stappen van functionaliteiten die pas in de latere paragrafen worden beschreven. De getallen die bij de acties tussen haakjes staan, verwijzen naar de getallen in Figuur 2.

4.2.2. Standaardwerking – functioneel

De standaardwerking[15] van een nieuw geïnstalleerde Exchange-omgeving is als volgt.[16] E-mails die een eindgebruiker verzendt of ontvangt blijven onbeperkt in de mailbox staan (*Postvak IN*, *Verzonden items*, of een zelfgemaakte map). De verzonden en ontvangen berichten kunnen door de eindgebruiker worden aangepast, waarbij



Figuur 2. <u>Algemene</u> werkwijze Exchange met de stappen tussen ontvangst/ verzending en technische vernietiging. De verschillende functionaliteiten worden in het hele hoofdstuk toegelicht. (Afbeelding gebaseerd op documentatie Microsoft.)

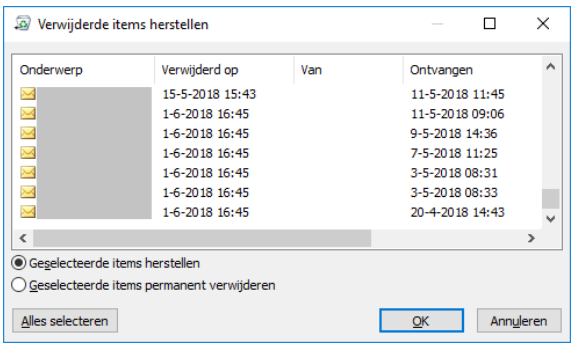
[14] Dit kan een generieke e-mailapplicatie zijn, of een door de IT-leverancier verschafte applicaties (zoals voor de klanten van SSC-ICT de BlackBerry-applicaties).
[15] Dus zonder gebruik te maken van de geavanceerdere functionaliteiten die in de volgende paragrafen staan.
[16] Wellicht ten overvloede: dit hoofdstuk beschrijft niet de huidige inrichting van Exchange bij SSC-ICT.

alleen de laatste (aangepaste) versie bewaard blijft. De eindgebruiker kan e-mails in de *Verwijderde items* ('prullenbak') plaatsen; ook die blijven onbeperkt bewaard. Als de eindgebruiker een e-mail uit de *Verwijderde items* verwijdert – of als de hele map *Verwijderde items* in één keer wordt geleegd (het legen van de prullenbak) – dan worden de betreffende e-mails na veertien dagen permanent vernietigd (technisch vernietigd). De eindgebruiker kan binnen die veertien dagen een e-mail nog terugzetten, of de e-mail alvast handmatig permanent verwijderen (technisch vernietigen). De e-mail kan dan niet meer worden gereconstrueerd.

4.2.3. Standaardwerking – technisch

(De getallen die tussen haakjes staan verwijzen naar de getallen in Figuur 2.) Een e-mail wordt ontvangen of verzonden, en komt in het *Postvak IN* of de *Verzonden items* (1). De eindgebruiker kan de e-mail verplaatsen naar een andere (zelfgemaakte) map. Als een eindgebruiker een e-mailbericht verwijdert (2), wordt het naar de map *Verwijderde items* verplaatst. E-mails in die map blijven, net als bijvoorbeeld in *Postvak IN*, onbeperkt[17] bewaard, totdat de eindgebruiker de e-mail ook uit die map verwijdert (3) (vergelijk het 'legen van de prullenbak'; dit gebeurt dus niet automatisch). De e-mail komt vervolgens in de map *Deletions*, die onderdeel is van de *Recoverable items*.

De map *Deletions* is (via Outlook) nog bereikbaar voor de eindgebruiker. Via het venster *Verwijderde items herstellen* kan de eindgebruiker de e-mail vervolgens terugzetten (stap 2 en 3 ongedaan maken). Via datzelfde venster kan de eindgebruiker ook kiezen voor 'permanent verwijderen'. In deze standaardwerkwijze is de e-mail dan ook permanent verwijderd (technisch vernietigd, de e-mail is dan niet meer te reconstrueren).[18] Zie ter illustratie in Figuur 3 hieronder het venster *Verwijderde items herstellen* met de opties herstellen en permanent verwijderen.



Figuur 3. Het venster Verwijderde items herstellen *in Outlook.*

[17] In deze paragraaf staat een algemene, gebruikelijke werking van Exchange-omgevingen. De werkwijze uit de *Handreiking* wijkt daarvan af op onder andere dit punt.

[18] Dat betekent dat de eindgebruiker een bericht permanent kan verwijderen voor de *deleted item retention period* is verstreken. De e-mail kan dan niet meer worden gereconstrueerd.

Ook zonder tussenkomst van de eindgebruiker, worden berichten in de map *Deletions* op een gegeven moment via een geautomatiseerd proces permanent verwijderd. Na afloop van de *deleted item retention period*[19] (standaard veertien dagen) wordt de e-mail namelijk verplaatst naar de map *Purges*. Vervolgens worden de items in die map *Purges* permanent verwijderd (technisch vernietigd) op het moment dat de *Managed Folder Assistant* (MFA) de mailbox verwerkt (6a). De MFA is een achtergrondproces dat op de Exchange-server draait, dat één voor één alle mailboxen verwerkt en de instellingen voor het bewaren en verplaatsen van berichten toepast. In de standaardinstelling, zorgt de MFA voor het permanent verwijderen (technisch vernietigen) van de e-mails die in de map *Purges* staan. De e-mail kan dan niet meer worden gereconstrueerd. De standaardinstelling is dat de MFA elke mailbox tenminste eens per dag verwerkt.[20]

4.3. Single item recovery (SIR)

4.3.1. Single item recovery – functioneel

Deze functionaliteit verandert de manier waarop verwijderde e-mails worden behandeld en kan alleen per mailbox aan of uit worden gezet. In de standaardwerking (paragraaf 4.2) is er een bepaalde periode (standaard veertien dagen) waarbinnen een verwijderde e-mail nog kan worden teruggezet, voordat de e-mail permanent wordt vernietigd. De eindgebruiker kan binnen die periode ook kiezen voor handmatige permanente verwijdering.
Dat laatste is niet meer mogelijk als de functionaliteit *Single item recovery* (SIR) voor de mailbox is ingeschakeld. Het bericht blijft dan tijdens die periode bewaard; de eindgebruiker kan het bericht dus niet handmatig permanent verwijderen.[21] Wel kan de eindgebruiker de e-mail geheel uit zijn zicht plaatsen, maar de beheerder kan de e-mail binnen die periode nog terughalen.

4.3.2. Single item recovery – technisch

Via het venster *Verwijderde items terugzetten van server* kan de eindgebruiker e-mails in de map *Deletions* terugzetten. De andere optie heet 'permanent verwijderen', maar heeft een ander effect als *SIR* is ingeschakeld. In dat geval wordt de e-mail (ondanks de tekst van de knop) niet permanent verwijderd, maar van de map *Deletions* verplaatst naar de map *Purges* (4a).
Wanneer de *Managed Folder Assistant* (MFA) de *Recoverable items map* verwerkt, wordt elk item in de map *Purges*

[19] De *deleted item retention period* is de periode waarin verwijderde items nog behouden blijven vanaf plaatsing in *Deletions*. De instelling geldt voor de gehele mailbox. Microsoft heeft deze standaard ingesteld op 14 dagen, maar dat is door de beheerder te wijzigen.
[20] Meer informatie is te vinden via deze link: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/recoverable-items-folder/recoverable-items-folder?view=exchserver-2019
[21] De eindgebruiker kan wel op een knop klikken met de (ongelukkig gekozen) tekst 'permanent verwijderen', waardoor het e-mailbericht geheel uit het zicht verdwijnt, maar de beheerder kan het toch terughalen.

geëvalueerd. Als de bewaarperiode (*deleted item retention period*) voor het bericht nog niet is verstreken, wordt het bericht niet verwijderd. Als de bewaarperiode voor het bericht wel is verlopen, wordt de e-mail automatisch permanent verwijderd (technisch vernietigd) (6a). De e-mail kan dan niet meer worden gereconstrueerd. Zo lang het bericht nog in de map *Purges* staat, kan het door tussenkomst van de beheerder worden teruggezet.[22]

4.4. Litigation Hold (LH)

4.4.1. Litigation Hold – functioneel

Als voor een mailbox *Litigation Hold* aan staat, blijft (deels "onder water", dat wil zeggen buiten het zicht van de eindgebruiker) alle inhoud van de mailbox behouden, inclusief verwijderde items en de oorspronkelijke versies van items die door de eindgebruiker zijn gewijzigd.
Deze functionaliteit kan alleen per mailbox aan of uit worden gezet. Een *Litigation Hold* kan op een mailbox worden geplaatst zonder dat de betreffende eindgebruiker daar iets van merkt.

4.4.2. Litigation Hold - technisch

De standaardinstelling in de Exchange-omgeving is dat *Litigation Hold* is uitgeschakeld: de eindgebruiker kan een oorspronkelijk e-mailbericht wijzigen, verwijderen en laten vernietigen.

Bij *Litigation Hold* kan optioneel een *hold duration* worden ingesteld: de bescherming van een item geldt dan binnen die tijdsperiode, die voor elk item wordt berekend vanaf het moment van ontstaan van het item (creatie/ontvangst van een e-mail). Zonder specifieke *hold duration* blijven items onder de hold oneindig bewaard.

Via het venster *Verwijderde items terugzetten van server* (zie Figuur 3 op pag. 20) kan de eindgebruiker e-mails in de map *Deletions* terugzetten. De andere optie heet weliswaar 'permanent verwijderen', maar heeft (net als bij *SIR*) een ander effect als voor de mailbox *Litigation Hold* is ingeschakeld. In dat geval wordt de e-mail (ondanks de tekst van de knop) niet permanent verwijderd, maar van de map *Deletions* verplaatst naar de map *Purges* (4a).

Wanneer de *Managed Folder Assistant* (MFA) de *Recoverable items map* verwerkt, wordt elk item in de map *Purges* geëvalueerd. Als de bewaarperiode (in dit geval dus de *hold duration*) voor het bericht nog niet is verstreken, wordt het bericht niet verwijderd uit de map *Purges*. Als de bewaarperiode (*hold duration*) voor het bericht wel is verlopen, wordt de e-mail automatisch permanent verwijderd

[22] Meer informatie is te vinden via deze link: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/recoverable-items-folder/recoverable-items-folder?view=exchserver-2019

(6a). Zo lang het bericht nog in de map *Purges* staat, kan het door tussenkomst van de beheerder worden teruggezet.

Als *Litigation Hold* wordt ingeschakeld, wordt ook automatisch *copy-on-write protection* aangezet voor de mailbox. Daarmee worden wijzigingen in berichten bijgehouden (zie paragraaf 4.6).

Als voor een mailbox *Litigation Hold* is ingeschakeld , dan geldt dat automatisch ook voor een eventueel aan de mailbox gekoppelde archiefmailbox (zie paragraaf 4.8).[23]

4.5. In-Place Hold (IPH)

4.5.1. In-Place Hold – functioneel

Met *In-Place Hold* kunnen specifieke e-mails behouden blijven, inclusief verwijderde items en de originele versies van gewijzigde items. Waar *Litigation Hold* per mailbox wordt ingesteld, geldt *In-Place Hold* per (afzonderlijk) e-mailbericht. De hold wordt geplaatst op de berichten die tijdens dat plaatsen voldoen aan de selectiecriteria die de beheerder opgeeft. Een criterium kan zijn dat een woord in een e-mail voorkomt, maar ook dat het een e-mail betreft die bijvoorbeeld voor een specifieke datum is ontvangen/verzonden. Een *In-Place Hold* kan op e-mailberichten in een mailbox worden geplaatst zonder dat de betreffende eindgebruiker daar iets van merkt.

4.5.2. In-Place Hold - technisch

De standaardinstelling in de Exchange-omgeving is dat *In-Place Hold* is uitgeschakeld: de eindgebruiker kan een oorspronkelijk e-mailbericht wijzigen, verwijderen en doen vernietigen.

Bij het plaatsen van een *In-Place Hold* geeft de beheerder aan voor welke mailboxen de hold geldt, aan welke zoekcriteria een e-mailbericht moet voldoen en optioneel hoe lang de e-mails moeten worden bewaard (*hold duration*). Er kunnen verschillende *In-Place Holds* per mailbox gezet worden. Berichten die na het plaatsen van de hold worden verstuurd of ontvangen, en die voldoen aan de zoekcriteria, worden ook onder de hold geplaatst. De zoekcriteria worden dus ook toegepast op nieuwe berichten. Voor elke wijziging in de zoekcriteria dient de *In-Place Hold* door de beheerder te worden vernieuwd.

Net als bij *Litigation Hold*, kan bij *In-Place Hold* optioneel een *hold duration* worden ingesteld: de bescherming van een item geldt dan binnen die tijdsperiode, die voor elk item wordt berekend vanaf het moment van ontstaan van het item (verzending/ontvangst van een e-mail). Zonder specifieke *hold duration* blijven items onder de hold oneindig bewaard.

[23] Meer informatie is te vinden via deze link: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/holds/holds?view=exchserver-2019

Via het venster *Verwijderde items terugzetten van server* (zie Figuur 3 op pag. 20) kan de eindgebruiker e-mails in de map *Deletions* terugzetten. De andere optie heet 'permanent verwijderen', maar heeft (net als bij *SIR* en *LH*) een ander effect als voor de mailbox *In-Place Hold* is ingeschakeld. In dat geval wordt de e-mail (ondanks de tekst van de knop) niet permanent verwijderd, maar van de map *Deletions* verplaatst naar de map *DiscoveryHold* (4b). Dit wijkt af van *SIR* en *LH*, waarbij de e-mail namelijk wordt verplaatst van *Deletions* naar *Purges*.

Wanneer de *Managed Folder Assistant* de map *Recoverable items* verwerkt, wordt elk item in de map *DiscoveryHold* geëvalueerd. Als de bewaarperiode (*hold duration*) voor het bericht nog niet is verstreken, wordt het bericht niet verwijderd. Als de bewaarperiode voor het bericht wel is verlopen, wordt de e-mail automatisch permanent verwijderd (6a). Zo lang het bericht nog in de map *DiscoveryHold* staat, kan het door tussenkomst van de beheerder worden teruggezet.

Als een *In-Place Hold* wordt ingeschakeld, wordt automatisch *copy-on-write protection* aangezet voor de mailbox. Daarmee worden wijzigingen in berichten bijgehouden (zie paragraaf 4.6).

Als voor een mailbox *In-Place Hold* is ingeschakeld, dan geldt dat automatisch ook voor een eventueel aan de mailbox gekoppelde archiefmailbox (zie paragraaf 4.8). [24]

4.6. Copy-on-write page protection

4.6.1. Copy-on-write page protection – functioneel

Zodra op een mailbox een *Litigation Hold* of een *In-Place Hold* wordt ingeschakeld, wordt automatisch de *copy-on-write page protection* ingeschakeld. De eindgebruiker kan dan nog steeds een verzonden/ontvangen e-mail wijzigen, maar buiten zijn zicht ("onder water") worden alle wijzigingen bijgehouden: *wat* er *wanneer* is gewijzigd.
Overigens houdt deze functionaliteit niet bij *wie* de e-mail heeft gewijzigd. Dat kan relevant zijn als een collega ook de rechten heeft om dat in de mailbox te doen.[25] Om dat bij te houden, kan aan *Audit logging* worden gedacht.[26]

4.6.2. Copy-on-write page protection – technisch

Zonder *copy-on-write page protection* kan een eindgebruiker een ontvangen/verzonden e-mail nog wijzigen, en blijft enkel en alleen de laatste (aangepaste) versie bewaard. Het origineel en eventuele tussenversies zijn dan verdwenen. Met

[24] Meer informatie is te vinden via deze link: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/holds/in-place-holds?view=exchserver-2019
[25] Denk aan functionele mailboxen, waar bijna altijd meer collega's bij kunnen. Maar denk ook aan managementassistenten met rechten op de mailbox van een manager.
[26] *Audit logging* wordt niet verder beschreven, omdat het niet relevant is voor de negen onderzochte eisen.

copy-on-write page protection – dat bij *IPH* en *LH* automatisch wordt ingeschakeld – wordt bij elke wijziging[27] van een e-mail een kopie van het oorspronkelijke item gemaakt voordat het gewijzigde item wordt weggeschreven. De kopie van het oorspronkelijke bericht wordt opgeslagen in de map *Versions* (binnen de *Recoverable items*). De map *Versions* is niet zichtbaar voor eindgebruikers. *Copy-on-write page protection* is van toepassing op items die zich in elk willekeurige map bevinden.[28]

4.7. Journaling

4.7.1. Journaling – functioneel

Journaling in Exchange Server maakt een kopie van in- en uitgaande e-mailberichten naar een speciale mailbox of naar een ander systeem.[29] In die mailbox (of dat andere systeem) staan dan duplicaten van de originele berichten: de eindgebruiker kan in zijn eigen mailbox berichten verwijderen of aanpassen, maar dat heeft geen invloed op de via journaling gekopieerde berichten.
Journaling vormt overigens geen oplossing voor de onderzochte eisen. Het kopiëren van berichten naar een ander systeem valt namelijk buiten de scope van de onderzoeksopdracht (zie paragraaf 2.4). Bovendien wordt de kopie meteen bij verzending/ontvangst van de e-mail gemaakt, zodat het met standaardfunctionaliteiten binnen Exchange niet mogelijk is om met *journaling* e-mails pas na 10 weken veilig te stellen.

4.7.2. Journaling – technisch

Tijdens de ontvangst/verzending van een e-mail wordt bij *journaling* een bericht met een kopie van de ontvangen/ verzonden e-mail als bijlage verstuurd naar een ingestelde *journaling mailbox* binnen of buiten de eigen Exchange-omgeving. Met *journal rules* kan worden ingesteld wat er wordt 'gejournald'. In de eerste plaats betreft dat van *wie* de berichten worden 'gejournald': iedereen binnen de organisatie, of specifieke personen of groepen daarbinnen. In de tweede plaats kan worden aangegeven of alleen e-mail binnen de eigen organisatie, alleen e-mail van/naar buiten de organisatie of álle e-mail wordt 'gejournald'. In de derde plaats kan de mailbox worden ingesteld waar de 'gejournalde' e-mails naartoe worden gestuurd.[30]

[27] Het betreft wijzigingen van het onderwerp, de hoofdtekst, de bijlagen, de verzenders, de ontvangers, en de verzend-/ontvangstdatum van een e-mail.
[28] Meer informatie is te vinden via deze link: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/recoverable-items-folder/recoverable-items-folder?view=exchserver-2019
[29] Het kopiëren van berichten naar een ander systeem valt buiten de scope van de onderzoeksopdracht. Zie paragraaf 2.4.
[30] Meer informatie is te vinden via deze link: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/journaling/journaling?view=exchserver-2019

4.8. Archive mailbox

4.8.1. Archive mailbox – functioneel

Een *archive mailbox* (archiefmailbox) is een aanvullende mailbox op de primaire mailbox van een eindgebruiker. Een *archive mailbox* functioneert als een extra set mappen om de data (e-mails) in op te slaan. De *archive mailbox* is via Outlook en Outlook on the web (voorheen: OWA, Outlook Web Access) toegankelijk. Eindgebruikers kunnen een *archive mailbox* inzien, en e-mail berichten verplaatsen of kopiëren tussen hun primaire mailbox en hun *archive mailbox*.
Een *archive mailbox* vormt overigens geen oplossing voor de onderzochte eisen. De relevante functionaliteiten van Exchange gelden óf tegelijkertijd voor zowel de reguliere mailbox als de *archive mailbox*, óf voor geen van beide. Voor een *archive mailbox* kan dus geen ander beleid gelden dan voor de reguliere mailbox.

4.8.2. Archive mailbox – technisch

Een *archive mailbox* is een tweede mailbox, compleet met eigen *Recoverable items*-mappen, die is gekoppeld aan de gewone (primaire/reguliere) mailbox. Als op de primaire mailbox een *Litigation Hold* of een *In-Place Hold* wordt ingesteld, wordt die automatisch ook op de *archive mailbox* ingesteld (en vice versa). Een *archive mailbox* is toegankelijk via Outlook en via Outlook on the web (voorheen: OWA, Outlook Web Access). Daarentegen is een *archive mailbox* technisch niet toegankelijk vanaf een andere client (mobiele e-mailapplicaties, zoals de BlackBerry-applicatie).[31]

4.9. Retention policy

4.9.1. Retention policy – functioneel

Met *retention policies* kan worden ingesteld dat berichten automatisch na een bepaalde periode (bijvoorbeeld tien jaar) worden vernietigd. Dit betekent niet impliciet dat de berichten ook gedurende die periode bewaard blijven, omdat de eindgebruiker de berichten handmatig eerder kan vernietigen. De beheerder kan een *retention policy* instellen voor een hele mailbox of enkele standaardmappen daarbinnen, door een default *retention policy* instellen. De eindgebruiker kan daar altijd van afwijken, door aan een bericht een *personal tag* toe te kennen en zo ervoor te zorgen dat een e-mail op een eerder of later moment (of nooit) wordt vernietigd. De door de eindgebruiker toegepaste *personal tag* 'wint' het van de door de beheerder ingestelde *retention policy*.

4.9.2. Retention policy – technisch

Microsoft Exchange biedt drie opties voor *retention tags*:
a. RPT (*Retention policy tag*): deze *tag* kan door de beheerder worden toegewezen aan standaardmappen in Exchange, zoals *Postvak IN* en *Verwijderde items*.

[31] Meer informatie is te vinden via deze link: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/in-place-archiving/in-place-archiving?view=exchserver-2019

b. DPT (*Default policy tag*): deze *tag* kan door de beheerder worden toegewezen aan items die geen *retention tag* hebben.
c. *Personal tag*: deze *tag* kan door de eindgebruiker worden toegewezen aan individuele e-mails en persoonlijke mappen.
Retention tags worden gebruikt om *retention settings* te zetten op mappen en e-mailberichten.

Een *retention policy* bestaat uit een groep van de hierboven beschreven *retention tags*. Een *policy* bevat dus instellingen voor standaardmappen, instellingen voor items die nog niet op een andere manier getagd zijn, en instellingen voor personal tags.

Een *retention tag* (RPT, DPT of *personal tag*) bestaat uit:
1. een naam voor de tag;
2. de *retention action*: met de drie opties *Delete and allow Recovery*, *Permanently Delete* en *Move to Archive* (zie toelichting hieronder).
3. de *retention period*: het moment waarop de actie moet worden uitgevoerd, gerekend in het aantal dagen vanaf verzending/ontvangst van de e-mail.

De MFA (zie paragraaf 4.2.3) verwerkt alle items in alle mailboxen en controleert of er op basis van de *retention tags* een actie moet worden ondernomen. Bij de actie *Delete and allow Recovery* wordt de betreffende e-mail verplaatst naar de map *Deletions* (onderdeel van de *Recoverable items*). Bij de actie *Permanently Delete* wordt de betreffende e-mail verplaatst naar de map *Purges*. Bij de actie *Move to Archive* wordt de betreffende e-mail verplaatst naar de *archive mailbox*.

De verschillende *tags* onderling werken als volgt samen.
Een *personal tag* krijgt altijd voorrang op een impliciete tag die de beheerder heeft gezet (RPT of DPT). Als een eindgebruiker een *personal tag* plaatst, kan deze een bericht zelf eerder verwijderen dan de (door de beheerder ingestelde) *policy tag* zou aangeven. Ook kan de eindgebruiker een *personal tag* plaatsen waardoor een bericht juist langer bewaard blijft. Ook is de *personal tag* 'Never Delete' mogelijk, zodat een bericht nooit door toepassing van een *retention tag* kan worden verwijderd.

De *retention tags* verschillen van de holds, omdat de *tags* geen bescherming bieden tegen eerder verwijderen door de eindgebruiker. De eindgebruiker kan een e-mail namelijk eerder verwijderen dan de beheerder met de *tags* had ingesteld. *Retention tags* kunnen wel in combinatie met de holds (IPH, LH) gebruikt worden. Met de *retention tags* wordt namelijk na een ingestelde periode een verplaatsing naar de map *Deletions* of *Purges* uitgevoerd.[32] Dat zou de eindgebruiker ook zelf hebben kunnen doen. De hold zorgt er vervolgens voor dat (conform de instellingen van die hold) de

[32] Of verplaatsing naar de archive mailbox, maar dat betreft geen verwijdering.

berichten niet worden vernietigd, maar in de map *Deletions* dan wel *Purges* blijven staan.[33]

4.10. Gevoeligheid van een bericht

4.10.1. Gevoeligheid van een bericht – functioneel

Bij het maken van een te verzenden e-mail, kan de eindgebruiker in Outlook een label meegeven aan de e-mail. Een voorbeeld van een regelmatig gebruikt label is een 'hoge urgentie'. Naast de urgentie, kan ook de gevoeligheid worden ingesteld: Normaal, Persoonlijk, Privé of Vertrouwelijk. Het effect is dat de ontvanger in Outlook boven de tekst van de e-mail een melding ziet: "Behandel dit als Persoonlijk" (of Privé/Vertrouwelijk, wat van toepassing is).

4.10.2. Gevoeligheid van een bericht – technisch

De gevoeligheid van een bericht is een eigenschap van de e-mail. Daarom kan de gevoeligheid van een e-mail alleen vóór de verzending worden ingesteld.[34]

[33] Meer informatie is te vinden via deze link: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mrm/retention-tags-and-retention-policies?view=exchserver-2019

[34] Bij een e-mail die een agenda-uitnodiging is, kan de gevoeligheid nog wel worden aangepast.

5. Technische oplossing per eis

5.1. Algemene bevindingen

5.1.1. Hold-functionaliteiten en compliance

De hold-functionaliteiten[35] zijn ontworpen om – vanuit (wettelijke) compliance-regels – het definitief verwijderen en aanpassen van oorspronkelijk berichten te voorkomen. Met de hold-functionaliteiten kan een juridisch geaccepteerd bewijs worden geleverd van de volledigheid en authenticiteit van het e-mailverkeer van en naar een mailbox. Daarom zijn deze functionaliteiten niet ontworpen om het mogelijk te maken om een e-mail te verwijderen in de eerste periode na verzending/ ontvangst. Wereldwijd worden de functionaliteiten van Exchange echter wel gebruikt om de volledigheid en authenticiteit van álle items binnen een mailbox te waarborgen en te bewijzen. Een hold kan zonder medeweten van de eindgebruiker worden geplaatst, wat in het algemeen nuttig is bij een integriteits- of opsporingsonderzoek. Daarom is het mogelijk dat berichten door de gebruiker zijn verwijderd, terwijl ze "onder water" – geheel buiten het zicht van de eindgebruiker – worden bewaard en technisch kunnen worden gereconstrueerd. Die berichten kunnen dan ook door de technisch beheerder worden opgeleverd bij informatie-verzoeken (zoals Wob-verzoeken).

5.1.2. Functionaliteiten ontworpen voor toepassing vanaf creatiedatum

De functionaliteiten van Exchange werken vanuit hun aard altijd aan de hand van kenmerken die gekoppeld zijn aan elk bericht. Een van die kenmerken is de creatiedatum: de verzend- of ontvangstdatum. Exchange kent geen enkele functionaliteit die is ontworpen om te ondersteunen dat tijdens een bepaalde periode (bijvoorbeeld de eerste tien weken na de creatiedatum) afwijkende regels gelden voor een bericht of de acties die daarop kunnen worden uitgevoerd. De functionaliteiten zijn ontworpen voor toepassing vanaf de creatiedatum.

5.1.3. Rollen binnen Exchange

Uit de *Interpretatie* volgt de wens dat de zorgdrager onder voorwaarden gegevens in mailboxen moet kunnen wijzigen en verwijderen. In Microsoft Exchange bestaat echter geen *functioneel beheerrol*, waarmee bijvoorbeeld een specifiek aangewezen en bevoegde medewerker van een ministerie handelingen[36] kan uitvoeren op de gegevens binnen de mailboxen van dat ministerie. De *eindgebruiker* heeft volledige beschikking over de eigen mailbox, met uitzondering van systeemmappen zoals de niet zichtbare delen van de map

[35] Litigation Hold en In-Place Hold. Zie paragraaf 4.4 en 4.5.
[36] Bij deze handelingen moet worden gedacht aan het aanmerken van een e-mail als privé, of het vernietigen van een e-mail na afloop van de tienwekentermijn. (Zie onder meer eis 8.)

Recoverable items. Geavanceerdere handelingen in de niet zichtbare delen, zoals het herstellen van items uit de map *Purges*,[37] kunnen alleen door de *technisch beheerder* worden uitgevoerd.[38]

5.1.4. Houdbaarheid van oplossingen op de lange termijn

De werkwijze uit de *Handreiking* bestrijkt lange termijnen, denk met name aan de tienjaarstermijn. Daarom is het van belang om bij de implementatie van de werkwijze te letten op de houdbaarheid van de oplossing. Microsoft biedt op dit moment ondersteuning voor twee versies die op een eigen server (in een eigen datacentrum) kunnen worden geïnstalleerd: Exchange Server 2016 en Exchange Server 2019. Beide versies worden ondersteund tot en met 14 oktober 2025. Microsoft heeft nog niet bekend gemaakt of er na Exchange Server 2019 nog een nieuwe versie komt die op een eigen server kan worden geïnstalleerd. Microsoft kan echter ook niet bevestigen dat Exchange Server 2019 de laatste versie waarbij dat kan. Microsoft biedt overigens wel als alternatief het afnemen van Exchange Online, een Cloud-dienst waarbij Exchange is geïnstalleerd op servers van Microsoft. Dit alternatief bestaat nu ook al, maar voor zover bekend wordt daar binnen de Rijksoverheid op dit moment geen gebruik van gemaakt.

Doordat de ondersteuning van Microsoft voor Exchange Server 2019 eindigt na 14 oktober 2025,[39] zal er al in de komende tien jaar een overgang naar een andere versie moeten plaatsvinden. Dat onderschrijft de noodzaak om gebruik te maken van functionaliteiten die standaardonderdeel zijn van Exchange: Het is uitermate waarschijnlijk dat die functionaliteiten ook in de volgende versies van Exchange worden opgenomen. Zelfgebouwde maatwerkaanpassingen aan Exchange zijn zeer waarschijnlijk niet compatibel met de volgende versies van Exchange.

Tijdens het onderzoek is overigens, ook wanneer dat niet expliciet in dit rapport is vermeld, steeds bij Microsoft gevraagd of Exchange Online (de Cloud-versie van Exchange) een functionaliteit biedt die (in het licht van dit onderzoek) meer oplossingen biedt dan de versies Exchange Server 2016 en 2019. Exchange Online verschilt namelijk van Exchange Server: het heeft onder andere een grotere capaciteit en rijkere functionaliteiten. Voor zover in ruime zin mogelijk relevant voor het onderzoek, biedt Exchange Online op dit moment geen andere of meer oplossingen dan Exchange Server voor de eisen die in dit onderzoek zijn onderzocht.

In de rest van dit hoofdstuk worden de technische oplossingen voor de negen onderzochte eisen beschreven, met daarbij de nadelen en risico's van die oplossing.

[37] Dit is overigens geen standaard dienstverlening van SSC-ICT.
[38] Daarvoor is een specifieke opdracht nodig van degene die daartoe bevoegd is.
[39] Zie https://support.microsoft.com/en-us/lifecycle/search/730.

5.2. Eis 1: E-mail wordt tien weken na ontvangst/verzending veiliggesteld

Deze eis is in de *Interpretatie* als volgt geformuleerd: E-mail wordt tien weken na ontvangst/verzending veiliggesteld.[40] In de praktijk is het misschien technisch niet mogelijk om dit op de seconde nauwkeurig tien weken na ontvangst/verzending van de e-mail te doen. Het veiligstellen mag dan ook batchgewijs zo snel mogelijk na afloop van de tienwekentermijn. (Zie paragraaf 4.2 van de *Interpretatie*.)

5.2.1. Technische oplossing

Met *In-Place Hold* (*IPH*, zie paragraaf 4.5) kan een beheerder items die aan een zoekopdracht (*query*) voldoen, in een hold zetten en die items daarmee veiligstellen. Met *IPH* kunnen alle items die (1) ouder zijn dan tien weken én (2) jonger zijn dan tien jaar, én (3) niet zijn uitgezonderd van veiligstellen, in een hold worden gezet.[41] De begindatum (1) en de einddatum (2) van de veilig te stellen berichten, verandert elke dag.[42] Dat betekent dat de query (zoekopdracht) elke dag moet worden aangepast.[43] Het uitzonderen van veiligstellen komt pas bij andere eisen aan de orde.

De technische werking van de *IPH* betekent concreet dat voor élk los item dagelijks moet worden gekeken naar de datum van verzending/ ontvangst.[44] De items die ouder zijn dan tien weken, maar jonger dan tien jaar, worden onder een hold (*IPH*) geplaatst met een *hold duration* van tien jaar. De eindgebruiker kan een e-mail dan wel volledig uit zijn zicht plaatsen, maar de berichten blijven "onder water" (in de map *Purges*) bewaard. Zij zijn beschikbaar als de beheerder informatie moet opleveren, bijvoorbeeld in het kader van een Wob-verzoek. Bij *IPH* worden ook de gewijzigde versies "onder water" bijgehouden, zodat de authenticiteit geborgd is.

In plaats van *IPH*, is ook *Litigation Hold* (*LH*, zie paragraaf 4.4) bekeken. Als *LH* wordt toegepast, worden alle e-mails meteen (na creatie/ontvangst) voor tien jaar veiliggesteld. Dan kunnen de e-mails in de eerste tien weken na verzending/ ontvangst dus niet worden uitgezonderd van het veiligstellen. Wel worden de gewijzigde versies "onder water"

[40] Het veiligstellen van een e-mail betekent dat gedurende een vastgestelde periode de oorspronkelijke e-mail niet kan worden vernietigd.
[41] Daarbij kan de hold worden beperkt tot items van een bepaald type: e-mail, taak, notitie, etc.
[42] Ook als het 'batchgewijs zo snel mogelijk na de tienwekentermijn' uit de eis wordt opgerekt tot een batch per week (en dus een wekelijks aangepaste query), gelden overigens de nadelen en risico's die in deze paragraaf 5.2 worden beschreven.
[43] Het is technisch niet mogelijk om de begin- en einddatum in 'formule-vorm' op te geven, bijvoorbeeld 'vandaag minus 70' (70 dagen = tien weken). Er moet een specifieke begin- en einddatum worden opgegeven.
[44] Bij een dagelijks aangepast query, kan het technisch niet anders dan dat alle items (dus ook dagelijks) moeten worden getoetst aan die query. Dit geldt overigens ook bij een andere aanpak, waarbij dagelijks een nieuwe hold wordt geplaatst op berichten die exact 10 weken oud zijn: dan moeten alsnog alle berichten worden beoordeeld op hun ouderdom. Daarbij wordt dan het maximumaantal gelijktijdige holds overschreden.

bijgehouden, zodat de authenticiteit geborgd is. Met *LH* is echter geen technische oplossing mogelijk voor deze eis.

Met *Single Item Recovery* (*SIR*, zie paragraaf 4.3) kunnen slechts de verwijderde berichten worden bewaard, maar worden de gewijzigde versies niet bewaard. Als de eindgebruiker een verzonden/ontvangen e-mail aanpast, wordt bij *SIR* de oorspronkelijke versie niet opgeslagen, maar alleen de laatst gewijzigde versie van het bericht. Ook kan *SIR* niet uitsluitend worden toegepast op items van tien weken of ouder: *SIR* staat óf aan voor de *gehele* mailbox, óf *SIR* is niet ingeschakeld. Ook *SIR* biedt daarom geen oplossing voor deze eis.

Het bovenstaande betekent dat aan de eis alleen kan worden voldaan door middel van *IPH*, waarbij dagelijks een gewijzigde query uitgevoerd wordt op alle items in alle mailboxen. Daaraan kleven de navolgende nadelen en risico's.

5.2.2. Nadelen

1. Microsoft kent geen enkele klant die *IPH* zo toepast (met een dagelijks aangepaste query op alle mailboxen) of die een soortgelijke werking beoogt. Exchange is niet ontworpen voor het gebruik van *IPH* op deze manier op deze enorme schaal (tienduizenden mailboxen) in combinatie met een dagelijks aangepaste query. Dat veroorzaakt allerlei nadelen en onzekerheden. Een hold is bedoeld om (meestal voor juridische doeleinden) de integriteit van de data te waarborgen of de correcte uitvoering van een werkproces binnen een organisatie te kunnen herleiden. Microsoft merkt op dat de tienwekentermijn, waarin de eindgebruiker deze data vrij mag aanpassen, niet in lijn is met een dergelijk oogmerk.

2. Door dagelijks een query te draaien (de berichten die aan de query voldoen in een hold te plaatsen), wordt een hoge dynamiek van de hold-functionaliteit (*IPH*) vereist. De Hold-functionaliteit is ontworpen voor een **statisch** scenario: over een lange periode moet data worden vastgehouden en op een later tijdstip worden geëxporteerd, geanalyseerd en verwerkt. De voorgestelde oplossing is volgens Microsoft dan ook een oneigenlijk gebruik van de Hold-functionaliteit. Microsoft Exchange is niet geoptimaliseerd voor een dergelijke **dynamische** toepassing en de gevolgen voor de gewone werking van Exchange zijn hierdoor niet bekend. Hoewel dit in een kleine proefomgeving waarschijnlijk goed zal functioneren, is de impact op een grootschalige implementatie (zoals die van SSC-ICT) niet te voorspellen. Exchange is namelijk niet ontworpen voor een scenario waarin dagelijks alle e-mail moet worden geraadpleegd. Daarnaast is Exchange sterk gebaseerd op een cachingmechanisme waarin een klein deel van de mailbox vaak wordt gebruikt en een relatief groot (oud) deel weinig wordt gebruikt. Geautomatiseerde processen die alle e-mail scannen – zoals de beschreven

toepassing van *IPH* – moeten dus met de nodige omzichtigheid worden ingezet. Door het toepassen van *IPH* worden de systemen mogelijkerwijs zwaarder belast. Dit betekent concreet:

a. Er is een zwaardere belasting van de Exchange-servers, zowel voor wat betreft de processoren, het aantal lees- en schrijfhandelingen op de harde schijven, de omvang van de opslag op die schijven en het gebruik van het werkgeheugen.
b. Doordat alle berichten elke dag moeten worden geëvalueerd, zullen alle berichten in het werkgeheugen (cache) worden bewaard. Exchange heeft een heel effectief cachingmechanisme waardoor de meeste geraadpleegde mail het snelst beschikbaar is. Bij het frequent doorlopen van alle mail zal dit cachingmechanisme mogelijkerwijs verstoord raken. Het gevolg is een overbelaste server, die slecht functioneert. Eindgebruikers zullen waarschijnlijk een trage server ervaren. Met name eindgebruikers die via een Citrixsessie werken, zullen worden geraakt.
c. Daarnaast zal de totale schijfruimte per mailbox toenemen. In de eerste plaats komt dat door de datagroei: er komt tien jaar lang alleen maar e-mail bij. Bovendien moet rekening worden gehouden met het volgende. Bij het aanzetten van *IPH* op een mailbox wordt het quotum voor de *Recoverable items* automatisch verhoogd tot 100 GB voor elke mailbox om de versies bij te houden van gewijzigde items.

Het gevolg van bovenstaande zwaardere belastingen is in ieder geval vertraging in het lezen, verzenden en ontvangen van e-mail door Exchange. Dit kan oplopen tot een lange vertraging die het regulier werken met e-mail verhindert. Microsoft wijst op de mogelijkheid om een verzoek om een Supportability Review in te dienen bij Microsoft, om de vraag naar de impact van een dagelijks aangepaste *IPH* voor te leggen aan de Exchange-productgroep. Omwille van de doorlooptijd van dit onderzoek is dat in overleg met de opdrachtgever niet in fase 1a gebeurd.

3. Het gevolg van de zwaardere belasting (zie hierboven onder 2a), is dat niet kan worden gegarandeerd dat de dagelijkse query/query's tijdig afgerond kan worden binnen het beschikbare tijdsvenster. De query's (en het bijbehorende plaatsen van de hold op de berichten die aan de query voldoen) vinden namelijk op de achtergrond plaats. Om te voorkomen dat een holdproces te veel impact heeft, wordt dat door het systeem met een hele lage prioriteit afgehandeld. Daarvoor wordt de capaciteit gebruikt die overblijft na de reguliere acties (het bekijken, verzenden en ontvangen van e-mail). De capaciteit die voor dit achtergrondproces beschikbaar is, is bovendien gemaximaliseerd omdat de reguliere acties prioriteit hebben. Elk bericht zal bij het draaien van de query geëvalueerd worden. De kans op een lange doorlooptijd van de query is groot. Door de beheerder kan niet worden gestuurd op de prioritering van het proces,

want dit gebeurt automatisch door het Exchange-platform. De *MFA* kan er bij drukte ook een week over doen, voordat alle mailboxen zijn doorgegaan. Daarom kan niet worden gegarandeerd dat de query-actie van de ene dag is afgerond, als de query-actie van de volgende dag al moet beginnen. Als de volgende query start, terwijl de vorige nog niet is afgerond, zorgt dat voor een steeds zwaardere belasting van het systeem, terwijl de holds niet meer op tijd (en uiteindelijk geheel niet meer) worden geplaatst. Het is namelijk onbekend of de dagelijkse aanpassing wordt verwerkt binnen een dag. Als dit niet het geval is zullen de holdverzoeken in een wachtrij worden geplaatst en mogelijkerwijs nooit worden gehonoreerd. Dan kan niet meer aan de eis worden voldaan.

4. Uit het voorgaande volgt dat het plaatsen van een hold, maar ook het opheffen ervan, niet plaatsvindt op een duidelijk aanwijsbaar moment. Het gevolg is dat mail die volgens de *Handreiking* had moeten worden veiliggesteld, dat nog (enkele dagen) niet is, terwijl dat niet zichtbaar is voor eindgebruikers en beheerders.[45]

5. Het is niet bekend en niet uit te rekenen hoeveel extra servers, werkgeheugen, opslag en processorkracht nodig zijn om deze functionaliteit in te schakelen op deze tienduizenden mailboxen. De schaling/rekensheets (storage calculator) van Microsoft zijn niet gemaakt (en kunnen dus geheel niet worden gebruikt) voor dit soort berekeningen, omdat Exchange nooit gemaakt is om op deze manier te worden gebruikt. Dat zorgt ervoor dat de financiële gevolgen niet kunnen worden ingeschat.

6. Voor de impact op stabiliteit, performance en de extra benodigde investering, kunnen (met aanvullende nadelen) inschattingen worden gemaakt door het te testen. Microsoft wijst erop dat deze oplossing in een kleine proefomgeving waarschijnlijk goed zal functioneren, maar dat de impact op een grootschalige implementatie zoals die van SSC-ICT niet is te voorspellen. De inschattingen en de testen geven dus geen garantie op een systeem dat op de lange termijn stabiel en zonder verstoringen blijft werken. Om de impact op een omgeving met onze omvang te testen, moet die test bovendien plaatsvinden in de live productie-omgeving. Dat betekent risico's voor de performance en stabiliteit van de productie-omgeving tijdens het testen. Daarbij is er geen separate back-up van de productie-omgeving.

7. Ook na het testen is over de tijd gezien geen zekerheid te behalen, omdat de omgeving dynamisch is. Onverwachte omstandigheden (zoals een dag waarop significant meer e-mail wordt verstuurd dan gemiddeld), kunnen op een later

[45] Dit levert strijd op met een eis die nu niet in dit onderzoek is onderzocht: "Het moment van veiligstellen moet wel duidelijk zijn voor de eindgebruiker en eenduidig kunnen worden gecommuniceerd. Het moet voor de eindgebruiker herkenbaar zijn wanneer een e-mail wel of niet veiliggesteld is." Zie par. 4.2 van de *Interpretatie*.

moment voor allerlei problemen zorgen op het gebied van performance en stabiliteit.

8. Microsoft biedt geen garantie op probleemoplossing, wel support met best effort. Microsoft kent geen klanten die hier ervaring mee hebben, dus Microsoft zelf heeft ook geen ervaring met het oplossen. De ondersteuning van Microsoft op Exchange Server 2016 en 2019 eindigt op 14 oktober 2025. Dat geldt dus ook voor een implementatie van deze oplossing, tenzij voor die tijd is gemigreerd naar een nieuwere (wel ondersteunde) versie van Exchange. Microsoft geeft nooit een garantie op een product, oplossing of implementatie, maar wel garantie voor een samen met de klant opgezette opzet, die volgens de richtlijnen van Microsoft is uitgevoerd.

9. Als op enig moment een verstoring in de Exchange-omgeving optreedt, heeft deze oplossing de omgeving zodanig complex gemaakt, dat het uitzoeken van de oorzaak van de verstoring en het opheffen daarvan bijna onmogelijk wordt.

Bovenstaande nadelen zijn niet te ondervangen door de omgeving op te delen in kleinere omgevingen, of door de omgeving te migreren naar Exchange Online.

5.2.3. Risico's

De risico's vloeien voort uit de nadelen. Zie daarom voorgaande paragraaf voor een toelichting op onderstaande risico's. (De nummering komt door aggregatie niet overeen met de nummering van de nadelen.)

1. Het oplossen van verstoringen door de beheerorganisatie wordt flink bemoeilijkt door de geïntroduceerde complexiteit in de configuraties en geautomatiseerde processen.
2. Microsoft stelt dat dit een oneigenlijk gebruik van de functionaliteit is. De ondersteuning van de leverancier bij het oplossen van problemen of verstoringen, is dus beperkt. Microsoft kent geen klanten met ervaring met deze implementatie.
3. De oplossing legt mogelijkerwijs een zware belasting op de Exchange-servers, met het risico dat eindgebruikers een zodanig vertraging merken in het lezen, verzenden en ontvangen van e-mail dat het reguliere werken met e-mail wordt verhinderd.
4. Met de beschreven oplossing is het niet zeker *wanneer* e-mails worden veiliggesteld en of dat *op tijd* gebeurt. Het niet tijdig veiligstellen is niet zichtbaar voor de beheerder en eindgebruiker.
5. Het is niet zeker dat de berichten *überhaupt* worden veiliggesteld, als de opdrachten van de ene dag nog niet zijn afgerond als die van de volgende dag al weer starten.
6. Het is niet bekend en niet uit te rekenen hoeveel extra servers, werkgeheugen, opslag en processorkracht nodig zijn. De performance calculator van Microsoft kan daar niet voor worden gebruikt. Dat betekend dat de financiële gevolgen van

het implementeren van deze oplossing op voorhand niet kunnen worden ingeschat.
7. Tijdens het testen in de live productie-omgeving is er verhoogde kans op verstoringen in de performance en stabiliteit van de gehele e-mailomgeving, wat het primair werkproces van de eindgebruikers serieus verstoort.
8. Ook is met testen in de productie-omgeving geen lange termijn zekerheid te behalen over de performance en stabiliteit van de hele Exchange-omgeving als deze oplossing wordt geïmplementeerd.

5.2.4. Tussenconclusie eis 1

Aan deze eis kan geheel worden voldaan door een *In Place Hold* toe te passen. De begin- en einddatum van de e-mails die onder de hold moeten vallen, zullen dagelijks moeten worden aangepast om de tienweken termijn te implementeren. Daaraan zijn serieuze nadelen en risico's verbonden (zie vorige paragrafen).

5.3. Eis 2: Veiliggestelde e-mails na tien jaar vernietigen

Deze eis is in de *Interpretatie* als volgt geformuleerd: E-mail die is veiliggesteld, wordt op een zeker moment vernietigd. Voor alle veiliggestelde e-mails zal die vernietiging plaatsvinden tien jaar na ontvangst/verzending van de e-mail. Het moment van vernietigen ligt niet per definitie direct/exact na afloop van de bewaartermijn van tien jaar. Het vernietigen zelf kost immers ook tijd. Het heeft de voorkeur dat de vernietiging niet te lang na afloop van de tienjaarstermijn plaatsvindt. Dat kan bijvoorbeeld in maandelijkse batches. (Zie paragraaf 6.1 en 6.3 van de *Interpretatie*.)

5.3.1. Technische oplossing

Met *IPH* (zie paragraaf 5.2.1) kan ervoor worden gezorgd dat een bericht *tijdens* de tienjaarstermijn niet kán worden verwijderd. Maar naast *IPH* is er nog iets anders nodig om ervoor te zorgen dat de berichten *ná* die tien jaar, ook echt worden verwijderd. Het opheffen van de bescherming van een bericht, is iets anders dan het daadwerkelijk verwijderen ervan.

De enige oplossing daarvoor bestaat uit het werken met een *retention policy*: alle items ouder dan tien jaar worden verwijderd (en verplaatst naar *Purges*). De *MFA* (zie paragraaf 4.2.3) zorgt voor de daadwerkelijke vernietiging op korte termijn daarna. Dit geldt voor alle berichten, zonder uitzondering (zie ook eis 9).
De eindgebruiker kan met eigen *retention tags* echter afwijken van de *retention policy*: daarmee kan een eindgebruiker op elk moment binnen de tienjaarstermijn een bericht dat na tien jaar vernietigd moet worden, toch nog aanmerken voor behouden, en zo die vernietiging voorkomen. Daarmee is niet technisch gewaarborgd dat alle veiliggestelde e-mails na tien jaar worden vernietigd. Deze oplossing is dan ook geen volledige oplossing voor deze eis.

Overigens biedt *Litigation Hold* in combinatie met een *retention policy* evenmin een oplossing. Dan wordt de e-mail onmiddellijk na creatie/ontvangst veiliggesteld en wordt niet aan eis 1 voldaan (zie paragraaf 5.2.1). Ook in dat geval kan een eindgebruiker met een eigen *retention tag* geautomatiseerde vernietiging na tien jaar voorkomen.

5.3.2. Nadelen

Voor *IPH* gelden dezelfde nadelen als hiervoor besproken bij eis 1 (zie paragraaf 5.2.2).
Daarnaast heeft het werken met een *retention policy* het nadeel dat de eindgebruiker met eigen *retention tags* kan afwijken van de *retention policy*: daarmee kan een eindgebruiker op elk moment binnen de tienjaarstermijn een bericht dat vernietigd moet worden, toch nog behouden. Daardoor is dit geen volledige oplossing voor deze eis.
Overigens kan de eindgebruiker een bericht, vanwege de *IPH*, niet eerder vernietigen dan na afloop van de hold (tien jaar).

5.3.3. Risico's

Voor *IPH* gelden dezelfde risico's als hiervoor besproken bij eis 1 (zie paragraaf 5.2.3).
Een *retention policy* heeft geen negatieve invloed op de performance van het systeem, aangezien de mail wordt gelabeld bij binnenkomst. Voor de verwijderactie wordt dus geen query gebruikt die dagelijks zou moeten worden geëvalueerd.

5.3.4. Tussenconclusie eis 2

Aan deze eis kan gedeeltelijk worden voldaan: veiliggestelde berichten kunnen na tien jaar automatisch worden vernietigd, maar de gebruiker kan dat echter voorkomen. Bovendien kent de gedeeltelijke oplossing serieuze nadelen en risico's.

5.4. Eis 3: Eindgebruiker kan e-mail vernietigen binnen tien weken na ontvangst/verzending

Deze eis is in de *Interpretatie* als volgt geformuleerd: In de eerste tien weken na ontvangst/verzending van de e-mail, kan de eindgebruiker de e-mail verwijderen. De verwijderde e-mail is daarna nog enige tijd terug te halen, voor het geval de eindgebruiker de e-mail abusievelijk heeft verwijderd. Daarna wordt de e-mail technisch vernietigd, wat betekent dat de inhoud van de e-mail niet meer kan worden gereconstrueerd. (Zie paragraaf 5.2 van de *Interpretatie*.)

5.4.1. Technische oplossing

Om vernietiging alleen binnen te tienwekentermijn mogelijk te maken, zou het handig zijn als de eindgebruiker (na die tien weken) een e-mail niet meer zou kunnen verplaatsen naar *Verwijderde items*. Exchange kent echter geen optie om het de eindgebruiker onmogelijk te maken een e-mail te verplaatsen naar de map *Verwijderde items*. Exchange kent evenmin een optie om het de eindgebruiker onmogelijk te

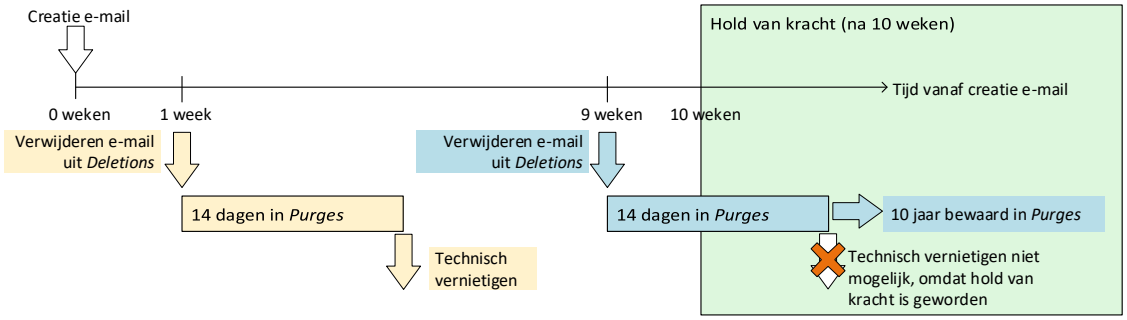
maken om een e-mail uit de *Verwijderde items* te verwijderen (vergelijk het legen van de prullenbak).[46] Die handelingen kunnen dan ook niet worden beperkt tot de eerste tien weken na ontvangst/verzending van een e-mail.
Wel kan met behulp van *IPH* het effect van die acties worden veranderd. De toepassing van *IPH* die in paragraaf 5.2 is beschreven, zorgt ervoor dat berichten die ná de tienweken-termijn door de eindgebruiker worden verwijderd, wel tien jaar bewaard blijven. Afhankelijk van de verwijderactie van de eindgebruiker, is dat mogelijk buiten het zicht van die eindgebruiker.[47] Op die manier kan (met alle in paragraaf 5.2 beschreven nadelen en risico's) worden bereikt dat e-mails die langer dan tien weken gelden zijn verzonden of ontvangen, behouden blijven.
De e-mails die in de afgelopen tien weken zijn ontvangen of verzonden, worden niet beschermd door de hold (*IPH*). Als *Single Item Recovery* (zie paragraaf 4.3) is uitgeschakeld, kan de eindgebruiker in de tienwekentermijn een bericht permanent vernietigen door deze uit de map *Deletions* te verwijderen. Dat bericht belandt dan niet in de map *Purges*, omdat het bericht nog niet wordt beschermd door de hold,[48] en wordt permanent vernietigd. Als de eindgebruiker het bericht in de map *Deletions* laat staan, zal het na verloop van tijd wel onder de hold komen te vallen en tien jaar lang niet kunnen worden vernietigd.

Met bovenstaande instelling (*IPH* ingeschakeld, *SIR* uitgeschakeld) wordt echter nog niet voldaan aan het tweede deel van deze eis. Een bericht dat binnen de tienwekentermijn wordt verwijderd uit *Deletions*, wordt immers meteen permanent vernietigd, en is niet enige tijd terug te halen (*SIR* staat immers uit). Om abusievelijk verwijderde berichten terug te kunnen halen, zal *Single Item Recovery* (*SIR*) moeten worden ingeschakeld. Zoals beschreven in paragraaf 4.3, moet bij *SIR* de *deleted item retention period* worden ingesteld: de periode waarbinnen een uit *Deletions* verwijderd bericht nog kan worden teruggehaald.

De werking van dat mechanisme kan het beste worden uitgelegd aan de hand van een voorbeeld. Stel dat de *deleted item retention period* wordt ingesteld op veertien dagen (twee weken). *SIR* is ingeschakeld, en *IPH* is ingeschakeld (op de manier die in paragraaf 5.2 uitgebreid is beschreven).

[46] Het is wellicht mogelijk om in de Outlook-client een of beide opties uit te schakelen. Daarbij is het echter ten eerste niet gegarandeerd dat volgende versies van de client die mogelijkheid blijven ondersteunen. Ten tweede hebben andere clients (zoals de BlackBerry-applicatie) ook toegang tot de Exchange-omgeving, en daarin kunnen deze opties niet worden uitgeschakeld. Door dus de optie op de meest gebruikte client uit te schakelen, kan niet worden gewaarborgd dat eindgebruikers de optie niet op een andere manier gebruiken.
[47] De eindgebruiker kan e-mails ook na de tienwekentermijn verwijderen uit de map *Verwijderde items* (prullenbak legen), en zelfs verwijderen uit de map *Deletions*. De berichten blijven dan echter uit het zicht van de eindgebruiker bewaard in de map *Purges* voor een periode van tien jaar.
[48] Het bericht is immers nog geen tien weken oud.

Berichten die na afloop van de tienwekenperiode worden verwijderd, blijven dan "onder water" in de map *Recoverable items* behouden door de *IPH*. Berichten die in de eerste tien weken na ontvangst/verzending worden verwijderd uit *Deletions*, blijven nog veertien dagen uit het zicht van de eindgebruiker bewaard in de map *Purges*. Berichten die in de eerste *acht*[49] weken na ontvangst/verzending worden verwijderd uit *Deletions* zullen veertien dagen na die verwijdering ook daadwerkelijk worden vernietigd. Voor die berichten wordt aan de eis voldaan. (Zie de geel gearceerde stroom in Figuur 4 hieronder.)
Maar voor de berichten die in de negende en tiende week na ontvangst/verzending worden verwijderd uit *Deletions*, is het effect anders. Ook deze berichten blijven nog veertien dagen in de map *Purges* staan, maar tijdens die veertien dagen, zullen zij onder de hold vallen. Immers tijdens die veertien dagen wordt het moment bereikt dat ze exact tien weken "oud" zijn. Op dat moment zullen ze worden beschermd door de hold, en tien jaar bewaard blijven. (Zie de blauw gearceerde stroom in Figuur 4 hieronder.)



Figuur 4. Samenloop van IPH en SIR.

Al met al zorgt de wens om de berichten nog veertien dagen te kunnen terughalen bij abusievelijke verwijdering, ervoor dat het verwijderen alleen in de eerste acht weken kan plaatsvinden.[50] Daarmee kan dus slechts gedeeltelijk aan de eis worden voldaan.[51]

5.4.2. Nadelen

1. De acties om een bericht daadwerkelijk in de eerste tien weken te verwijderen zijn niet gebruiksvriendelijk. Na het verwijderen uit de gewone map, moet de e-mail ook nog uit de *Verwijderde items* worden verwijderd, en daarna ook uit de map *Deletions* (zie Figuur 3 in paragraaf 4.2.3).
2. Die laatste stap kan niet met een mobiele applicatie zoals de BlackBerry-applicatie worden uitgevoerd, maar alleen via Outlook.

[49] Tien weken minus de veertien dagen *deleted item retention period*.
[50] De twee weken/veertien dagen is een voorbeeld om de werking uit te leggen, en verder nergens op gebaseerd. Als dat drie weken/21 dagen wordt, dan verandert de acht weken ook in zeven weken.
[51] Overigens kan met *Litigation Hold* geheel niet aan de eis worden voldaan. De e-mail valt dan vanaf het moment van creatie al onder de hold, zodat het onmogelijk is dat de eindgebruiker de e-mail in de eerste tien weken verwijdert.

3. Uit de vorige paragraaf volgt dat aan de eis niet volledig kan worden voldaan. Óf verwijderen is tijdens de hele tienwekentermijn mogelijk, maar een vergissing kan niet worden hersteld. Verwijderen is dan onmiddellijk permanent. Óf een abusievelijk verwijderde e-mail kan nog enige tijd worden hersteld, maar dan is het verwijderen niet tijdens de *gehele* tienwekentermijn mogelijk. In dat geval is de functionele werking gecompliceerder, en dus minder eenvoudig uit te leggen aan eindgebruikers.
4. Aan het gebruik van *IPH* kleven ook de nadelen die al in paragraaf 5.2.2 zijn beschreven.

5.4.3. Risico's

Aan het gebruik van *IPH* kleven ook de risico's die al in paragraaf 5.2.3 zijn beschreven. Daarnaast bestaat het risico dat de werkwijze zodanig gecompliceerd is dat de eindgebruiker zich vergist in de uitvoering: de eindgebruiker kan vergeten álle noodzakelijke handelingen te verrichten die voor vernietiging noodzakelijk zijn, waardoor het bericht abusievelijk toch wordt veiliggesteld. Of de eindgebruiker kan vergeten dit tijdig te doen, omdat het een actie vereist vóór het aflopen van de tienwekentermijn. Deze werkwijze is niet gebruikersvriendelijk. Daarmee staat deze oplossing op gespannen voet met een van de wensen die nu niet is onderzocht (zie eis A in bijlage 3): "Het is in het algemeen wenselijk als de hele werkwijze voor de eindgebruiker zo intuïtief mogelijk werkt."

5.4.4. Tussenconclusie eis 3

Aan de eis kan niet volledig worden voldaan. Óf verwijderen is tijdens de hele tienwekentermijn mogelijk, maar een vergissing bij het verwijderen kan niet worden hersteld. Óf een abusievelijk verwijderde e-mail kan nog enige tijd worden hersteld, maar dan is het verwijderen niet tijdens de *gehele* tienwekentermijn mogelijk. Beide opties hebben serieuze nadelen en risico's.

5.5. Eis 4: Terughalen verwijderde e-mail binnen tienwekentermijn

Deze eis is in de *Interpretatie* als volgt geformuleerd: Binnen de tienwekentermijn moet een (abusievelijk) verwijderde e-mail nog kunnen worden teruggehaald, zodat de verwijdering ongedaan gemaakt wordt. De verwijderde e-mail mag dus pas na afloop van de tienwekentermijn technisch worden vernietigd. (Zie paragraaf 5.2 van de *Interpretatie*.)

5.5.1. Technische oplossing

De technische oplossing voor deze eis staat beschreven in paragraaf 5.4.1. Deze eis voegt aan de vorige eis toe dat een e-mail die op een zeker moment tijdens de tienwekentermijn is verwijderd gedurende het nog resterende deel van de tienwekentermijn nog moet kunnen worden teruggehaald, en dat de permanente verwijdering (technische vernietiging) pas plaatsvindt na afloop van de tienwekentermijn.

Uit de beschrijving van paragraaf 5.4.1 volgt dat aan deze eis niet kan worden voldaan.[52] Een hold geldt voor alle berichten die tien weken of ouder zijn, dus de gewenste permanente verwijdering moet vóór het verstrijken van de tienwekentermijn plaatsvinden. Daarna kan dat niet meer. Ook de combinatie van *SIR* met *IPH*, die in paragraaf 5.4.1 staat, voldoet niet aan deze eis. Daarmee wordt slechts tijdens een deel van de tienwekentermijn (en niet de gehele tienwekentermijn) mogelijk gemaakt om berichten terug te halen.

5.5.2. *Tussenconclusie eis 4*
Er is geen technische oplossing voor deze eis.

5.6. **Eis 5: Terughalen verwijderde e-mail nog korte tijd na tienwekentermijn mogelijk**
Deze eis is in de *Interpretatie* als volgt geformuleerd: Die technische vernietiging mag onmiddellijk na afloop van die tienwekentermijn plaatsvinden. Het heeft echter de voorkeur als een verwijderd bericht ook na de tienwekentermijn nog een korte tijd behouden blijft, en pas na die korte tijd technisch wordt vernietigd. Dan is het namelijk mogelijk om binnen die korte tijd na afloop van de tienwekentermijn een (abusievelijk) verwijderde e-mail nog terug te halen. Die korte tijd kan nader worden bepaald en ligt in de orde van grootte van een paar weken, zodat die korte tijd in verhouding staat tot de tienwekentermijn. (Zie paragraaf 5.2 van de *Interpretatie*.)

5.6.1. *Technische oplossing*
In paragraaf 5.5.1 (in samenhang met paragraaf 5.4.1) is al uiteengezet dat het niet mogelijk is om e-mail die binnen de tienwekentermijn is verwijderd, pas na afloop van die tienwekentermijn te vernietigen.

5.6.2. *Tussenconclusie eis 5*
Er is geen technische oplossing voor deze eis.

5.7. **Eis 6: Eindgebruiker kan e-mail binnen tien weken na ontvangst/verzending aanmerken als privé**
Deze eis is in de *Interpretatie* als volgt geformuleerd: Een eindgebruiker kan een e-mail binnen tien weken na ontvangst/verzending aanmerken als privé. Deze functionaliteit is bedoeld om het mogelijk te maken dat niet-relevante e-mail wordt uitgezonderd van veiligstellen. (Zie paragraaf 5.3 van de *Interpretatie*.)

5.7.1. *Technische oplossing*
Voor het aanmerken van e-mails als privé, zijn vier opties overwogen:
1) verplaatsen e-mail naar map met de naam “privé”;

[52] Als er geen hold wordt gezet, en geen enkel bericht wordt veiliggesteld, kan strikt genomen wel aan de eis worden voldaan. Maar dan wordt niet meer aan eis 1 en 2 voldaan en zijn berichten niet voor tien jaar veiliggesteld.

2) plaatsen van *retention tag* "privé (Never delete)" op de e-mail;
3) e-mail indelen in een categorie "privé", en
4) e-mail markeren met gevoeligheid "privé" of "persoonlijk".

Opties 1, 2 en 3 zijn altijd mogelijk en kunnen technisch niet worden beperkt tot de eerste tien weken na creatie van de e-mail. De eindgebruiker kan deze opties te allen tijde toepassen (mits ze zijn aangezet).

Optie 4 kan alleen op het moment dat een e-mail wordt verzonden door de eindgebruiker worden ingesteld. Deze optie werkt dus niet bij ontvangen mail en kan niet ná het moment van verzending alsnog worden toegepast.

Overigens kunnen opties 2, 3 en 4 alleen worden ingesteld via Outlook en niet via elke mobiele applicatie (zoals de BlackBerry-applicatie).

Uit de eis volgt dat als privé aangemerkte e-mails niet mogen worden veiliggesteld. Dat betekent dat ze dus niet onder de hold van *IPH* moeten vallen (zie paragraaf 5.2.1). Het is echter technisch niet mogelijk om álle eigenschappen van een e-mail te gebruiken bij de selectie van wat wel en wat niet onder de hold moet vallen.[53] Van de vier genoemde opties kan alleen optie 3 (categorie "privé") worden ingesteld als criterium voor *IPH*.

Dat betekent dat met optie 3 kan worden voldaan aan deze eis: De eindgebruiker kan een e-mail in Outlook categoriseren in een categorie "privé".[54]

5.7.2. Nadelen

Een e-mail kan via de Outlook-client op de reguliere digitale werkomgeving de categorie "privé" krijgen. Dat is echter niet mogelijk via de mobiele applicatie (zoals BlackBerry).[55]
Deze oplossing kent geen risico's.

5.7.3. Tussenconclusie eis 6

Er is een technische oplossing voor deze eis.

5.8. Eis 7: Eindgebruiker kan na tien weken e-mail niet meer als privé aanmerken

Deze eis is in de *Interpretatie* als volgt geformuleerd: Het moet onmogelijk zijn voor de eindgebruiker zelf om een

[53] Het is bij IPH wel mogelijk om berichten te selecteren die juist *niet* aan een bepaalde voorwaarde voldoen. In dit geval betreft dat berichten die *niet* de categorie "privé" hebben.
[54] Deze eis betreft het binnen tien weken kunnen aanmerken als privé; deze eis betreft niet het *enkel en alleen* binnen tien weken kunnen aanmerken als privé. Dat een bericht ná tien weken niet meer als privé moet kunnen worden aangemerkt, is een andere eis (eis 7).
[55] Het is niet onderzocht en daarmee niet uitgesloten dat er mobiele applicaties bestaan waarbij dit wel mogelijk is.

veiliggestelde e-mail na de tienwekentermijn[56] alsnog als privé aan te merken. (Zie paragraaf 4.4 van de *Interpretatie*.)

5.8.1. Technische oplossing

Het is technisch onmogelijk om het aanmerken als privé te limiteren tot de eerste tien weken (zie paragraaf 5.7.1). Als een eindgebruiker een e-mail na de tienwekentermijn categoriseert als "privé", zal die e-mail bij de volgende keer dat de *IPH* wordt toegepast (dagelijks, zie paragraaf 5.2.1) niet meer in de hold vallen. Daarmee is die e-mail niet meer veiliggesteld, en (in strijd met de eis) nog na de tienwekentermijn als privé aangemerkt.[57]

5.8.2. Tussenconclusie eis 7

Er is geen technische oplossing voor deze eis.

5.9. **Eis 8: Zorgdrager kan na tien weken e-mail nog wel vernietigen of als privé aanmerken**

Deze eis is in de *Interpretatie* als volgt geformuleerd: Het moet echter wel mogelijk zijn dat de zorgdrager aan de ICT-leverancier een opdracht geeft om een veiliggestelde e-mail na de tienwekentermijn alsnog te vernietigen, of als privé aan te merken. (Zie paragraaf 4.4 van de *Interpretatie*.)

5.9.1. Technische oplossing

Ten aanzien van het kunnen aanmerken als privé van een veiliggestelde e-mail:
De eindgebruiker kan *altijd* een bericht aanmerken als privé (zie paragraaf 5.7.1). Uit paragraaf 5.7.1 volgt dat de enige oplossing voor het aanmerken als privé is de toepassing van een categorie: de eindgebruiker wijst een categorie "prive" toe aan een bericht. In dat geval – waarbij de eindgebruiker overigens ook na de tienwekentermijn nog een e-mail als privé kan aanmerken – is het mogelijk dat een beheerder (steeds in opdracht van de zorgdrager) een bericht aanmerkt als privé door tijdelijk verhoogde rechten op de mailbox van de eindgebruiker te krijgen.

Ten aanzien van het kunnen vernietigen van een veiliggestelde e-mail:
Deze eis betekent dat een e-mail die onder een hold valt, moet kunnen worden vernietigd. Bij beide typen holds (*LH* en *IPH*) moet de hold dan tijdelijk worden opgeheven voordat de vernietiging kan plaatsvinden. Dat zou betekenen dat eerst de mailbox moet worden geïsoleerd, zodat de eindgebruiker

[56] De tienwekentermijn betreft de eerste tien weken na het moment van ontvangst/verzending van een e-mail. Elke e-mail heeft een eigen tienwekentermijn.

[57] Het moment waarop een bericht een categorie krijgt toegewezen, wordt niet bijgehouden. Daarop kan niet worden geselecteerd. Ook is het niet mogelijk om het beschreven probleem te omzeilen door dagelijks een nieuwe hold te plaatsen op de berichten die exact tien weken oud zijn. Weliswaar zou dan een wijziging na die tien weken geen effect meer hebben op de hold, maar het maximumaantal holds is niet toereikend om tien jaar dagelijks een nieuwe hold te plaatsen. (Zie ook voetnoot 44.)

tijdelijk geen toegang meer heeft tot zijn mailbox gedurende de tijd dat de hold van de mailbox af is. Daarna moet de hold worden opgeheven. Vervolgens kan de beheerder full access op de mailbox krijgen en het specifieke bericht(en) verwijderen in het bijzijn van de zorgdrager (vier-ogen-principe). Daarna wordt de hold weer opnieuw geplaatst, wordt de full access van de beheerder ingetrokken, en krijgt de eindgebruiker weer toegang tot zijn mailbox.

Het gevolg is echter dat te veel e-mails permanent worden vernietigd, ook e-mails die absoluut niet mogen worden vernietigd. Op het moment dat de hold wordt opgeheven, zullen namelijk automatisch alle berichten in de map *Purges* worden vernietigd. (Zie verder het eerste nadeel hieronder). Dit gevolg is zo zwaarwegend (en in strijd met eis 1), dat met deze oplossing dus niet aan de eis kan worden voldaan.

5.9.2. Nadelen

Ten aanzien van het kunnen aanmerken als privé van een veiliggestelde e-mail:
Nadat een beheerder een bericht alsnog als privé heeft aangemerkt, kan de eindgebruiker dat eenvoudigweg ongedaan maken.

Ten aanzien van het kunnen vernietigen van een veiliggestelde e-mail:
1. Op het moment dat de hold wordt opgeheven, zullen alle berichten in de map *Purges* worden vernietigd. Dat is niet tegen te houden of te voorkomen. Sterker nog: dat is het mechanisme waarmee het specifieke te verwijderen bericht ook zal worden vernietigd. Het gevolg is dus dat enerzijds het te vernietigen bericht netjes wordt vernietigd, maar dat anderzijds ook een onbekend aantal berichten die moeten zijn veiliggesteld, permanent worden vernietigd.
2. De uitvoering van de oplossing is nogal complex en omslachtig.
3. De actie zal in een beschikbaar tijdsvenster, waarschijnlijk buiten kantoortijden, moeten worden uitgevoerd door de beheerder in het bijzijn van de zorgdrager (vier-ogen-principe).
4. De uitvoering zal in overleg met de eindgebruiker moeten worden gepland, omdat tijdens het proces de mailbox niet beschikbaar is voor de eindgebruiker.

5.9.3. Risico's

Ten aanzien van het kunnen vernietigen van een veiliggestelde e-mail:
1. Als er ook maar één item in de map *Purges* staat op het tijdstip dat de hold er vanaf gaat, dan zal dat item worden vernietigd, terwijl het zou moeten zijn veiliggesteld. Veiliggestelde e-mail zal dus ook worden verwijderd, dat is niet te voorkomen. Het is niet te voorkomen dat een eindgebruiker een item in *Purges* kan plaatsen.

2. Het kan niet worden uitgesloten dat de eindgebruiker toch bij zijn mailbox kan als de hold wordt opgeheven. Dan kan de eindgebruiker berichten vernietigen, terwijl die berichten zouden moeten zijn veiliggesteld.
3. Er is een kans op fouten bij de technische uitvoering, doordat het complex en omslachtig is. De actie is namelijk handmatig en niet-geautomatiseerd. Als per ongeluk het verkeerde bericht wordt verwijderd, is dat onomkeerbaar.

5.9.4. Tussenconclusie eis 8

Voor een deel van deze eis (veiliggestelde e-mail alsnog aanmerken als privé) bestaat een technische oplossing die nadelen kent. Voor het andere deel van deze eis (veiliggestelde e-mail alsnog vernietigen) is er geen technische oplossing.

5.10. Eis 9: Als privé aangemerkte e-mails worden niet na tien jaar automatisch vernietigd

Deze eis is in de *Interpretatie* als volgt geformuleerd: E-mails die zijn uitgezonderd van veiligstellen door ze als privé aan te merken, worden niet vernietigd, omdat ze niet zijn veiliggesteld. (Zie paragraaf 6.2 van de *Interpretatie*.)

5.10.1. Technische oplossing

In paragraaf 5.7.1 staan vier opties voor het aanmerken van e-mails als privé. Bij opties 1, 3 en 4 (mapje, categorie, gevoeligheid) heeft het aanmerken als privé geen invloed op het moment van vernietiging. En alleen optie 3 (categorie) voldoet aan eis 6.
Als op een mailbox een *retention policy* geldt waarbij alle e-mails na tien jaar worden verplaatst naar *Deletions*, dan geldt dat ook voor de e-mails die op een van die drie manieren zijn aangemerkt als privé. Dat betekent dat privé-berichten ook worden vernietigd. Dat is dus geen oplossing voor deze eis.

In paragraaf 5.7.1 is nog een andere optie beschreven voor het aanmerken als privé (optie 2): De eindgebruiker kan een *retention tag* "privé (Never Delete)" op de e-mail plaatsen om die e-mail uit te zonderen van het verwijderen/ vernietigen. Het plaatsen van zo'n *tag* kan altijd, en kan niet worden beperkt tot de eerste tien weken na verzending/ontvangst van de e-mail (zie paragraaf 5.7.1 en 5.3.2). Het gevolg van een Never Delete tag, is dat het bericht nooit[58] wordt verwijderd, dus ook niet na tien jaar, tenzij de gebruiker de *tag* weer verwijdert.

Dat betekent dat om aan deze eis 9 én aan eis 6 te voldoen, een bericht als privé kan worden aangemerkt door zowel:

[58] Van elke eindgebruiker eindigt ooit het dienstverband. Dan heeft die eindgebruiker ook geen toegang meer tot de als privé aangemerkte berichten. Op enig moment zullen ook de als privé aangemerkte berichten met de hele mailbox worden verwijderd. Zie de wens in paragraaf 6.2 van de *Interpretatie*. Dat betreft geen onderzochte eis, dus daar wordt in dit tussenrapport niet verder op ingegaan.

- het bericht de categorie “privé” toe te wijzen (eis 6), én
- een *retention tag* “privé (Never Delete)” op het bericht te plaatsen.

Dit vereist twee afzonderlijke handelingen per bericht van de eindgebruiker.

5.10.2. Nadelen

Een serieus nadeel is de complexiteit voor de eindgebruiker. Om een bericht als privé aan te merken, moet de eindgebruiker namelijk twee afzonderlijke handelingen verrichten: een categorie én een *retention tag* toepassen op het bericht. Daarmee staat deze oplossing op gespannen voet met een van de wensen die nu niet is onderzocht (zie eis A in bijlage 3): “Het is in het algemeen wenselijk als de hele werkwijze voor de eindgebruiker zo intuïtief mogelijk werkt.” De enige oplossing voor deze eis is het gebruik van de *retention tag* “privé (Never Delete)”, maar daarmee wordt niet meer voldaan aan eis 7, zie paragraaf 5.8.

Daarbij kan ook met deze oplossing niet aan eis 7 worden voldaan. De *retention tag* kan namelijk op elk moment, dus ook ná de tienwekentermijn, nog worden toegepast op een e-mail. Op deze manier kan veiliggestelde mail op elk moment worden uitgezonderd van vernietiging door de eindgebruiker.

5.10.3. Risico’s

Het risico bestaat dat de werkwijze zodanig gecompliceerd is dat de eindgebruiker zich vergist in de uitvoering: de eindgebruiker kan vergeten *beide* noodzakelijke handelingen te verrichten die noodzakelijk zijn voor het aanmerken als privé. Daardoor wordt ofwel het bericht abusievelijk toch veiliggesteld, ofwel het bericht abusievelijk na afloop van de tienjaarstermijn automatisch vernietigd. Deze werkwijze is niet gebruikersvriendelijk.

5.10.4. Tussenconclusie eis 9

De enige technische oplossing kent een serieus risico, omdat het gecompliceerd is voor de eindgebruikers. De oplossing voldoet niet aan eis 7.

6. Conclusie

6.1. Onderzoeksresultaten

De uitkomsten zijn samengevat weergegeven in onderstaande tabel. Daarin staat achtereenvolgens weergegeven: een korte samenvatting van de eis, of een technische oplossing mogelijk is met de standaardfunctionaliteiten van Microsoft Exchange, en of er nadelen en risico's aan de oplossing kleven. Daarbij is eis 8 opgesplitst in 8a en 8b. Alleen als een oplossing helemaal voldoet aan een eis, wordt deze met een vink aangegeven. De oplossing bij eis 2 en 3 voldoet slechts gedeeltelijk aan de eis en is daarom met een kruis weergegeven.

Eis	Technische oplossing in Microsoft Exchange	Nadelen en risico's
Eis 1: E-mail wordt tien weken na ontvangst/verzending veiliggesteld	✔ Mogelijk	✘ Serieuze nadelen en risico's
Eis 2: Veiliggestelde e-mails na tien jaar vernietigen	✘ Gedeeltelijk mogelijk	✘ Serieuze nadelen en risico's
Eis 3: Eindgebruiker kan e-mail vernietigen binnen tien weken na ontvangst/verzending	✘ Gedeeltelijk mogelijk	✘ Serieuze nadelen en risico's
Eis 4: Terughalen verwijderde e-mail binnen tienwekentermijn	✘ Geheel niet mogelijk	
Eis 5: Terughalen verwijderde e-mail nog korte tijd na tienwekentermijn mogelijk	✘ Geheel niet mogelijk	
Eis 6: Eindgebruiker kan e-mail binnen tien weken na ontvangst/verzending aanmerken als privé	✔ Mogelijk	
Eis 7: Eindgebruiker kan na tien weken e-mail niet meer als privé aanmerken	✘ Geheel niet mogelijk	
Eis 8a: Zorgdrager kan na tien weken e-mail nog wel vernietigen	✘ Geheel niet mogelijk	
Eis 8b: Zorgdrager kan na tien weken e-mail nog wel als privé aanmerken	✔ Mogelijk	✘ Serieuze nadelen
Eis 9: Als privé aangemerkte e-mails worden niet na tien jaar automatisch vernietigd	✔ Mogelijk	✘ Serieuze nadelen en risico's

Voor zover een oplossing (deels) mogelijk is, betreffen de geïdentificeerde risico's daarvan onder meer (niet uitputtend):

- De stabiliteit van de e-mailomgeving kan niet worden gegarandeerd;
- Voor veel eindgebruikers kan het regulier werken met e-mail worden verhinderd, als gevolg van oplopende vertragingen in het lezen, verzenden en ontvangen van e-mail;
- Er is een verhoogde kans op verstoringen die ook nog eens lastiger zijn te verhelpen, temeer omdat Microsoft geen enkele klant kent die een soortgelijke oplossing heeft geïmplementeerd;
- Performancetesten geven zelfs geen zekerheid van stabiliteit op de lange termijn;

- Vooraf kunnen de financiële gevolgen van een implementatie niet worden ingeschat, doordat van tevoren niet kan worden bepaald hoeveel extra hardware en beheerinspanning benodigd is;
- De implementatie (voor zover mogelijk) is zo gecompliceerd, dat de werking en werkwijze niet eenvoudig kan worden uitgelegd aan de eindgebruikers.

6.2. Conclusie

Uit het onderzoek blijkt dat de werkwijze uit de *Handreiking* niet kan worden geïmplementeerd met de standaard-functionaliteiten binnen Microsoft Exchange. Voor het merendeel van de onderzochte negen eisen blijkt namelijk geen technische oplossing binnen de standaardfunctionaliteiten binnen Microsoft Exchange te bestaan. Voor enkele eisen bestaat wel een technische oplossing, maar die oplossingen gaan echter gepaard met serieuze nadelen en risico's voor onder meer de stabiliteit en betrouwbaarheid van de e-maildienstverlening aan de eindgebruikers. Deze conclusie zal overigens ook niet wijzigen als uit fase 1b eventueel zou blijken dat voor alle overige eisen een technische oplossing wel volledig mogelijk zou zijn zonder nadelen of risico's.[59]

[59] De opdracht van het onderzoek heeft zich beperkt tot het vinden van oplossingen binnen de standaardfunctionaliteiten van Microsoft Exchange. Andere mogelijke oplossingen zijn daarom niet onderzocht. Daarbij kan worden gedacht aan oplossingen waarbij ook andere software dan strikt alleen Microsoft Exchange wordt gebruikt, of aan procesmatige of organisatorische oplossingen. Uit dit onderzoek kan dus nadrukkelijk niets worden afgeleid over de mogelijkheden om de werkwijze uit de Handreiking op een andere wijze te kunnen implementeren.

Bijlage 1. Handreiking bewaren van e-mail Rijksoverheid

Bewaren van e-mail Rijksoverheid

Handreiking

Inhoudsopgave

Bewaren van e-mail Rijksoverheid

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 Assessment (PIA) en het uitvoeren van de volgende onderzoeken door het Nationaal Archief:

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

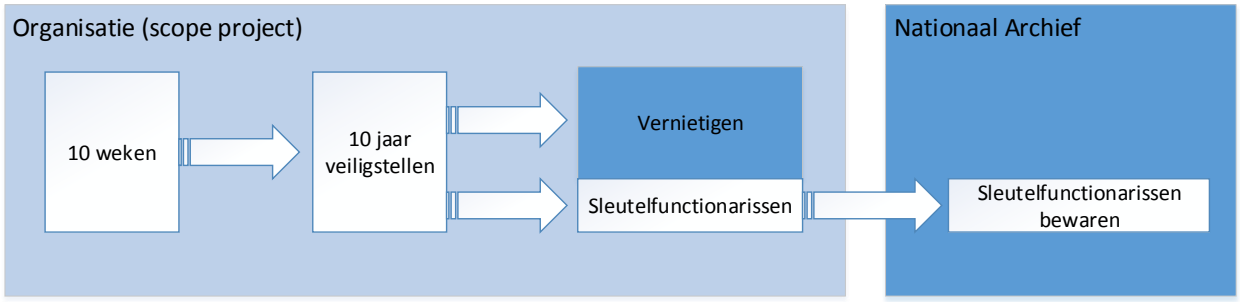
De handreiking is bedoeld voor organisaties van de Rijksoverheid.

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 sleutelfunctionarissen en overige e-mail die als blijvend te bewaren is aangemerkt naar het Nationaal Archief overgebracht. Bij overbrenging kunnen organisaties openbaarheidsbeperkingen 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 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-mailberichten 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 sleutelfunctionarissen 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 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 informatie-verzoek. Het is daardoor van belang te zorgen voor goede software om het zoekproces te onder-steunen.

8.2 Bedrijfsvoering

Organisaties zijn in eerste instantie slechts gehouden om toegang te verstrekken indien informatie-verzoeken 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 informatie-verzoeken.

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.

Bijlage 2. Interpretatie van de Handreiking bewaren van E-mail Rijksoverheid

SSC-ICT
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Interpretatie van de Handreiking bewaren e-mail Rijksoverheid

Versie	1.0
Datum	17 december 2019
Status	Definitief

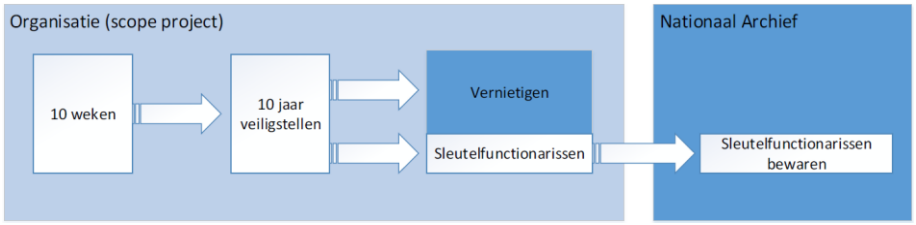
Inhoud

1. Inleiding

In de *Handreiking Bewaren van e-mail Rijksoverheid* (hierna: *Handreiking*) staat de werkwijze voor het bewaren van e-mail beschreven. SSC-ICT verricht in opdracht van het Rijksprogramma voor Duurzaam Digitale Informatiehuishouding (hierna: RDDI) een onderzoek naar de technische oplossingsrichtingen om die werkwijze mogelijk te maken. De onderzoeksopdracht heeft betrekking op de technische oplossings-richtingen binnen de shared Microsoft Exchange-omgeving van SSC-ICT. Het heeft daarbij de voorkeur zoveel mogelijk gebruik te maken van standaardfunctionaliteiten. Van het shared e-mailplatform op basis van Microsoft Exchange – dat toegankelijk is vanaf de werkplek via Outlook en vanaf een smartphone of tablet via een BlackBerry-applicatie – maken op dit moment vijf departementen gebruik (BZK, FIN, IenW, SZW en VWS).

Aangezien de Handreiking niet het karakter heeft van een functioneel ontwerp is een nadere interpretatie van de uitgangspunten van de Handreiking naar technische eisen en wensen nodig om het onderzoek uit te kunnen voeren. In het kader van dit onderzoek is daarom tijdens enkele bijeenkomsten door een vertegenwoordiging van SSC-ICT en RDDI[1] een nadere interpretatie aan de *Handreiking* gegeven. Aan de hand van de uitkomsten van deze bijeenkomsten is dit document opgesteld. Deze interpretatie is opgesteld ten behoeve van het onderzoek: aan de hand van dit stuk wordt de reikwijdte bepaald en een concreet kader beschreven waarbinnen de technische oplossingsrichtingen moeten worden gezocht.

De werkwijze die in de *Handreiking* staat beschreven, kan worden opgedeeld in vier hoofdfunctionaliteiten:
(1) het **Veiligstellen** van alle e-mails voor een periode van tien jaar;
(2) het **Uitzonderen van veiligstellen** van specifieke e-mails in de eerste tien weken;
(3) het **Vernietigen** van de veiliggestelde e-mails na tien jaar en;
(4) het **Overdragen** van een deel van de e-mails aan het Nationaal Archief na tien jaar.



Figuur 1. Werkwijze E-mail bewaren. (Bron: Handreiking E-mail bewaren Rijksoverheid.)

Het onderzoek is opgedeeld in fase 1a en 1b. Dit document is opgesteld ten behoeve van fase 1a, waarin technische oplossingsrichtingen worden

[1] In de bijlage staat een lijst met deelnemers aan één of meerdere vooroverleggen over de interpretatie van de *Handreiking* voor dit onderzoek.

onderzocht voor een *minimale invulling van de Handreiking*. Tot dat te onderzoeken minimum worden de drie hoofdfunctionaliteiten *Veiligstellen*, *Uitzonderen van veiligstellen* en V*ernietigen* gerekend. De mate waarin voor deze drie hoofdfunctionaliteiten technische oplossingsrichtingen worden gevonden, is bepalend om tot fase 1b van het onderzoek over te gaan (go/no go door opdrachtgever RDDI). De drie functionaliteiten vormen aldus het minimum om die beslissing te kunnen nemen. Als in fase 1a wordt geconcludeerd dat technische oplossingsrichtingen mogelijk zijn, betekent dat overigens niet dat die oplossingsrichtingen per definitie ook in fase 1b mogelijk zijn.

In fase 1b wordt een *volledige invulling* van de *Handreiking* onderzocht, inclusief de hoofdfunctionaliteit *Overdragen* en enkele aanvullende eisen in het kader van duurzame toegankelijkheid, waaronder een onderzoek naar de mogelijkheden om de e-mail te doorzoeken. In dit document wordt steeds expliciet aangegeven welke functionaliteiten bij fase 1b zullen worden betrokken; zonder expliciete vermelding vormen de functionaliteiten onderdeel van onderzoeksfase 1a.

In het volgende hoofdstuk wordt het begrippenkader beschreven. Het is aan te bevelen eerst dit hoofdstuk te lezen alvorens men de daaropvolgende hoofdstukken tot zich neemt. Na het begrippenkader volgt een hoofdstuk met algemene opmerkingen over de interpretatie van de werkwijze in de *Handreiking* en de scope van het onderzoek. In de hoofdstukken 4,5 en 6 wordt de interpretatie van de drie hoofdfunctionaliteiten *Veiligstellen*, *Uitzonderen van veiligstellen* en *Vernietigen* uitgebreid besproken.

Het onderhavige document betreft een tussenproduct van onderzoeksfase 1a. Het geheel van fase 1a zal worden afgerond met een tussenrapport.

2. Begrippenkader

Dit begrippenkader verduidelijkt de begrippen die in de volgende hoofdstukken worden gebruikt. Deze lijst is opgesteld ten behoeve van het onderzoek en omvat alleen de begrippen die daarvoor nodig zijn. Dat betekent dat in dit hoofdstuk niet alle begrippen en aspecten van de *Handreiking* worden behandeld. Zie daarvoor de producten die het project E-mailarchivering van RDDI heeft opgeleverd.[2]

De begrippen in dit hoofdstuk verwijzen soms naar elkaar. Daarom zijn ze in een logische volgorde geplaatst en niet alfabetisch.

2.1. E-mail

Onder e-mail wordt verstaan e-mailberichten inclusief eventuele bijlagen.

2.2. Eindgebruiker

Een eindgebruiker is de persoon die uiteindelijk de e-maildienstverlening gebruikt. Elke medewerker met een e-mailaccount is dus een eindgebruiker.

2.3. Archiefbescheiden

Archiefbescheiden zijn informatie (-objecten) gebonden aan de werkprocessen van het overheidsorgaan.[3] Veiliggestelde e-mails hebben de status van archiefbescheiden.

2.4. Zorgdrager

Een zorgdrager is degene die bij of krachtens de (Archief)wet belast is met de zorg voor de archiefbescheiden.[4] Dat betekent ook dat de zorgdrager beslist over wat er met veiliggestelde e-mails gebeurt. Bijvoorbeeld: het bepalen van de bewaartermijn, uitzonderen van veiligstellen, vernietigen, of overbrengen van e-mails. De zorgdrager voor een veiliggestelde e-mail blijft de zorgdrager voor die e-mail; ook als de betreffende eindgebruiker bij een ander rijksonderdeel (een andere zorgdrager) komt te werken.

2.5. Sleutelfunctionaris

De zorgdrager bepaalt welke van zijn functionarissen worden aangewezen als sleutelfunctionaris.[5] Het uitgangspunt is dat de topformatie (ABD Topstructuur) als sleutelfunctionaris wordt aangemerkt. Daarnaast kunnen andere sleutelfunctionarissen worden aangewezen. Conform de termijn daarvoor gesteld in de Archiefwet wordt e-mail van sleutelfunctionarissen naar het Nationaal Archief overgebracht. Bij overbrenging kunnen organisaties openbaarheidsbeperkingen aanbrengen.

---

[2] Die producten zijn niet bij dit onderzoek betrokken.

[3] Zie https://www.nationaalarchief.nl/archiveren/kennisbank/archiefbescheiden

[4] Zie https://www.nationaalarchief.nl/archiveren/kennisbank/zorgdrager

[5] Op dit moment is in opdracht van RDDI een *Handleiding aanwijzing en beheer sleutelfunctionarissen* in ontwikkeling. Die zal na voltooiing kunnen worden gedownload via de site van RDDI: www.informatiehuishouding.nl.

2.6. Hotspot

Een hotspot is een gebeurtenis of kwestie die leidt tot een opvallende of intensieve interactie tussen overheid en burgers, of tussen burgers onderling.[6] Het gaat om zaken die veel maatschappelijke beroering veroorzaken. Een voorbeeld is MH17. E-mails over hotspots worden overgebracht naar het Nationaal Archief, zie paragraaf 3.8 en 6.5.

2.7. Authentiek informatieobject

Een authentiek informatieobject is een informatieobject waarvan kan worden bewezen: a) dat het is wat het beweert te zijn; b) dat het opgemaakt of verzonden is door de persoon die beweert het te hebben opgemaakt of verzonden, en c) dat het opgemaakt of verzonden is op het tijdstip als aangegeven.[7]

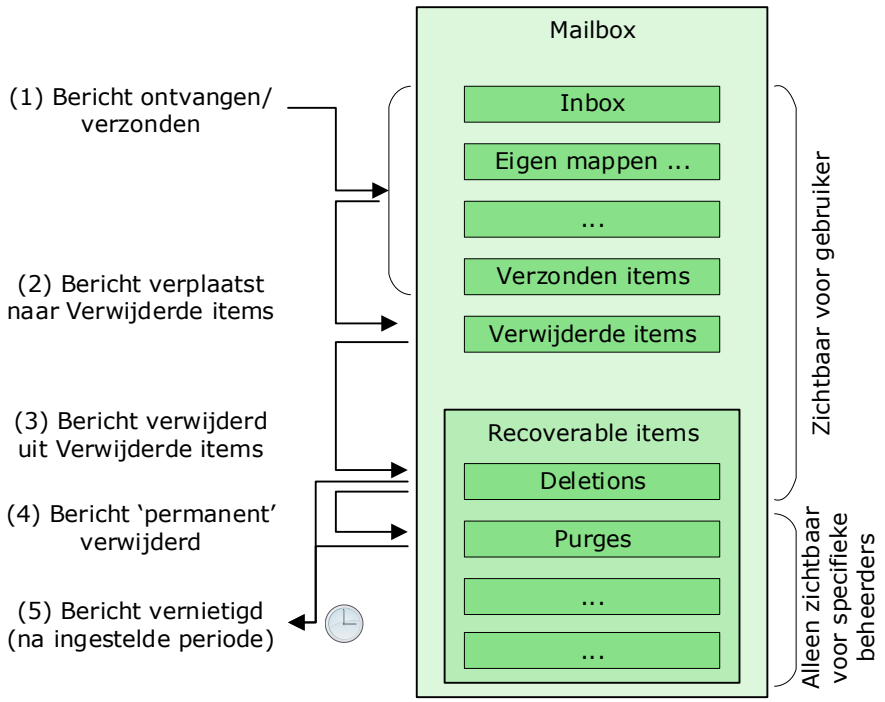
2.8. Oorspronkelijke e-mail

Een oorspronkelijke e-mail is de e-mail zoals die is ontvangen/verzonden en die voldoet aan de eisen aan een authentiek informatieobject. Als een e-mail na ontvangst/verzending is aangepast, is die e-mail niet meer gelijk aan de oorspronkelijke e-mail en daarmee niet meer authentiek.

2.9. Verwijderen

In dit document betekent 'verwijderen' de actie van de eindgebruiker om e-mail in de map *Verwijderde items* te plaatsen. De e-mail is daarmee *niet* technisch vernietigd. Om het verschil tussen verwijderen en technisch vernietigen duidelijk te maken, is een **algemene beschrijving** van de werking van Exchange-omgevingen op dit punt nodig. In de volgende illustratie zijn de stappen weergegeven die een e-mail in een standaard Exchange-omgeving aflegt van ontvangst/verzending tot technische vernietiging. Deze toelichting betreft de algemene werking in een Exchange-omgeving, en betreft niet (een implementatie van) de werkwijze uit de *Handreiking*.

[6] Zie https://www.nationaalarchief.nl/archiveren/kennisbank/handreiking-waardering-en-selectie
[7] Zie https://www.nationaalarchief.nl/archiveren/kennisbank/authentiek-informatieobject



Figuur 2. <u>Algemene</u> werkwijze Exchange met de stappen tussen ontvangst/verzending en technische vernietiging. (Afbeelding gebaseerd op documentatie Microsoft.)

Als een eindgebruiker een e-mailbericht verwijdert (2), wordt het naar de map *Verwijderde items* verplaatst. E-mails in die map blijven, net als bijvoorbeeld in de *Inbox*, onbeperkt[8] bewaard, totdat de eindgebruiker de e-mail ook uit die map verwijdert (3) (vergelijk het 'legen van de prullenbak', dit gebeurt dus niet automatisch). De e-mail komt vervolgens in de map *Deletions*, die onderdeel is van de *Recoverable items*. Die map *Deletions* is nog bereikbaar voor de eindgebruiker.
Via de knop *Verwijderde items terugzetten van server* kan de eindgebruiker de e-mail vervolgens terugzetten, of kiezen voor 'permanent verwijderen' (4). Als hij/zij kiest voor 'permanent verwijderen', dan is de e-mail geheel niet meer zichtbaar voor de eindgebruiker. De e-mail is verplaatst naar een andere map (*Purges*) binnen *Recoverable items* die alleen voor een klein aantal specifieke beheerders toegankelijk is. Nadat de e-mail een bepaalde (in te stellen) periode in een *Recoverable items* map heeft gestaan, wordt de e-mail definitief verwijderd ('technisch vernietigd, zie paragraaf 2.10') (5) uit de e-mailomgeving.

Zoals eerder vermeld, betekent 'verwijderen' in dit document de actie van de eindgebruiker om e-mail in de map *Verwijderde items* te plaatsen (dus nummer (2) in de illustratie). De verwijderde e-mail zal in de meeste gevallen dus nog bestaan en teruggehaald kunnen worden. Verwijderen is immers niet hetzelfde als technisch vernietigen.

[8] In deze paragraaf staat een algemene, gebruikelijke werking van Exchange-omgevingen in het algemeen. De werkwijze uit de *Handreiking* wijkt op dit punt daarvan af. Die werkwijze staat pas in de volgende hoofdstukken beschreven.

2.10. Technisch vernietigen

Onder technisch vernietigen wordt verstaan dat de e-mail wordt gewist uit de e-mailomgeving (Exchange-omgeving) en daaruit niet meer kan worden gereconstrueerd. Dat betreft stap nummer (5) in de illustratie van de vorige paragraaf. De informatie van het e-mailbericht kan nog steeds geheel of gedeeltelijk buiten de e-mailomgeving bestaan (bijvoorbeeld in een afdruk op papier). Dit betreft dus het vernietigen vanuit de techniek bezien, wat anders is dan het vernietigen in de zin van de Archiefwet (zie paragraaf 2.11).

2.11. Vernietigen

Vernietigen zoals in de *Handreiking* vermeld, is een term uit de Archiefwet. Vernietigen is het proces dat leidt tot het technisch vernietigen of wissen van veiliggestelde e-mails (archiefbescheiden), zodat zij niet weer gereconstrueerd kunnen worden. Zie ook hoofdstuk 6.

'Vernietigen' omvat dus het hele proces,[9] terwijl 'technisch vernietigen' slechts betrekking heeft op het niet-reconstrueerbaar maken (wissen) van de gegevens. Een ander onderscheid is dat 'vernietigen' alleen gaat om veiliggestelde e-mail, terwijl 'technisch vernietigen' betrekking heeft op *alle* e-mails (veiliggesteld en niet-veiliggesteld).

2.12. Veiligstellen

Het veiligstellen van een e-mail betekent dat de oorspronkelijke e-mail gedurende een vastgestelde periode niet kan worden vernietigd. Voor de volledigheid wordt opgemerkt dat met de term "veiligstellen" in de Handreiking niet wordt gedoeld op voorzieningen (zoals back-ups) om gegevens bij een calamiteit weer terug te kunnen zetten, opdat het primaire werkproces kan worden hervat. Het veiligstellen in de *Handreiking* en deze interpretatie heeft betrekking op het authentiek en beschikbaar houden van de gegevens ten behoeve van verschillende soorten informatieverzoeken en overdracht aan het Nationaal Archief. Zie ook hoofdstuk 4.

2.13. Tienwekentermijn

De tienwekentermijn betreft de eerste tien weken na het moment van ontvangst/verzending van een e-mail. Elke e-mail heeft een eigen tienwekentermijn.

2.14. Tienjaarstermijn

De tienjaarstermijn betreft de eerste tien jaar na het moment van ontvangst/verzending van een e-mail. Elke e-mail heeft een eigen tienjaarstermijn.

2.15. Niet-relevante e-mails

Niet-relevante e-mails zijn de e-mails die binnen de tienwekentermijn mogen worden uitgezonderd van veiligstellen. Niet-relevante e-mails zijn bijvoorbeeld privé e-mail, p-vertrouwelijke zaken of e-mail niet uit hoofde van functie verstuurd of ontvangen. Zie hoofdstuk 5 voor het uitzonderen van veiligstellen.

[9] Dat proces omvat bijvoorbeeld ook het opstellen van een verklaring van vernietiging.

3. Algemeen

3.1. Ruim kader voor het onderzoek

Voor dit onderzoek geldt in het algemeen dat de technische oplossingsrichtingen moeten worden gezocht binnen deze interpretatie van de Handreiking. Het doel is het vinden van een of meerdere oplossingsrichtingen die aan álle eisen en wensen voldoen.

Om een zo volledig mogelijk beeld te geven, mogen echter ook oplossingen worden onderzocht die niet volledig aan alle eisen voldoen. Daarbij wordt in het rapport dan aangegeven in welke mate aan de eisen kan worden voldaan. Het is immers op voorhand niet ondenkbaar dat sommige eisen niet verenigbaar zijn: als aan de ene eis wordt voldaan, kan wellicht technisch niet meer aan de andere eis worden voldaan en andersom. Door bij het onderzoeken en het opstellen van het rapport dit ruimere kader te hanteren, wordt de bruikbaarheid van het rapport als basis voor nadere besluitvorming vergroot.

3.2. Herkenbaarheid en gebruiksvriendelijkheid

Het is in het algemeen wenselijk als de hele werkwijze voor de eindgebruiker zo intuïtief mogelijk werkt en er voor de eindgebruikers zo min mogelijk verandert aan de huidige interfaces (Outlook en BlackBerry) en werkwijze. De eindgebruiker moet bovendien op een eenvoudige manier het onderscheid kunnen herkennen tussen de volgende drie categorieën e-mails: (1) veiliggestelde e-mails, (2) e-mails die zijn uitgezonderd van veiligstellen en (3) e-mails die niet zijn veiliggesteld én niet zijn uitgezonderd. In deze derde categorie zitten de e-mails die nog geen tien weken oud zijn en dus nog niet zijn veiliggesteld, terwijl deze e-mails ook (nog) niet door de eindgebruiker zijn uitgezonderd van veiligstellen.

3.3. Tijdstip van ontvangst/verzending bij doorgestuurde of beantwoorde e-mail

Bij het doorsturen of beantwoorden van een e-mail, of door een e-mail als bijlage bij een andere e-mail te voegen, wordt een eerdere e-mail opnieuw verzonden. Daarmee ontstaat een nieuw e-mailbericht, met een nieuw ontvangst-/verzendtijdstip, en voor dat nieuwe e-mailbericht gaan de termijnen (tien weken, tien jaar) opnieuw lopen.

3.4. Uitgezonderde mailboxen

Het moet technisch mogelijk zijn om in opdracht van de zorgdrager (functionele) mailboxen uit te zonderen van de toepassing van de werkwijze van de *Handreiking*. Voor die uitgezonderde mailbox kan de zorgdrager met de ICT-leverancier andere afspraken maken. Dit kan bijvoorbeeld gewenst zijn voor de (functionele) mailbox van een integriteitscoördinator of een bedrijfsarts, maar maakt het bovendien mogelijk om de werkwijze binnen een departement gefaseerd in te voeren. In het onderzoek moet naar voren komen wat de technische consequenties zijn van het maken van dit soort uitzonderingen.

3.5. Functionele postbussen

Functionele postbussen of groepspostbussen zijn mailboxen die niet gekoppeld zijn aan (een account van) een eindgebruiker, maar het zijn mailboxen waar meerdere eindgebruikers voor zijn geautoriseerd, bijvoorbeeld secretariaatspostbussen. Voor dit onderzoek wordt geen onderscheid gemaakt tussen een functionele postbus en een reguliere mailbox van een eindgebruiker. Dat betekent bijvoorbeeld ook dat de eindgebruikers die toegang hebben tot een functionele postbus, op dezelfde manier e-mails kunnen uitzonderen van veiligstellen (zie hoofdstuk 5).

Sommige functionele postbussen worden niet door eindgebruikers gebruikt, maar voor het geautomatiseerd ontvangen en verwerken van berichten in bijvoorbeeld een zaaksysteem. Die vallen niet onder de *Handreiking*, omdat de archivering van die berichten al elders (in het zaaksysteem) is belegd. Dat sluit aan op de vorige paragraaf: technisch moeten aangewezen functionele postbussen kunnen worden uitgezonderd van de toepassing van de werkwijze van de *Handreiking*.

3.6. Inactieve mailboxen

De werkwijze van de *Handreiking* moet ook voor inactieve mailboxen gelden. Dat zijn mailboxen die zijn gedeactiveerd en daarom geen e-mail meer kunnen ontvangen/verzenden. Een mailbox wordt bijvoorbeeld gedeactiveerd omdat de eindgebruiker uit dienst is gegaan of bij een ander departement is gaan werken. Ook functionele postbussen die niet meer worden gebruikt, kunnen worden gedeactiveerd.

Het bovenstaande betekent onder andere dat het proces van vernietigen van veiliggestelde e-mails na de tienjaarstermijn ook geldt ook voor inactieve mailboxen (zie hoofdstuk 6). Bovendien moet het ook bij een inactieve mailbox mogelijk zijn om in opdracht van de zorgdrager na de tienwekentermijn veiliggestelde e-mail alsnog uit te zonderen van veiligstellen of deze vóór de tienjaarstermijn al te vernietigen (zie paragraaf 4.4 en 6.4).

3.7. Sleutelfunctionarissen en register

De e-mail van sleutelfunctionarissen wordt tien jaar na ontvangst/ verzending overgebracht naar het Nationaal Archief. Voor sleutelfunctionarissen geldt dat het veiligstellen en het uitzonderen van veiligstellen hetzelfde werkt als voor andere eindgebruikers. Het vernietigen van hun e-mail geschiedt logischerwijs pas ná succesvolle overdracht aan het Nationaal Archief.

Per organisatie wordt een register van sleutelfunctionarissen ingericht. De verantwoordelijkheid voor het actueel houden van het register ligt bij de zorgdrager zelf. Bijzondere aandacht is nodig voor naamswijzigingen[10] van sleutelfunctionarissen: bij een naamswijziging in het register of bij wijziging van het e-mailadres is het van belang dat de koppeling tussen beide in stand blijft.

[10] Een naam kan bijvoorbeeld door een huwelijk wijzigen. Soms wordt dan ook het e-mailadres gewijzigd.

3.8. Overdracht bij niet-sleutelfunctionarissen

De zorgdrager kan bepalen dat, naast de e-mails van sleutelfunctionarissen, ook e-mails van niet-sleutelfunctionarissen moeten worden overgebracht naar het Nationaal Archief. Dat kan onder andere in het geval van een *hotspot*. De hoofdfunctionaliteit *Overdragen* wordt in fase 1b onderzocht.

3.9. Oplossingen in een centrale Exchange-omgeving

In het onderzoek worden technische oplossingsrichtingen onderzocht op de shared Exchange-omgeving van SSC-ICT. Daarmee is het uitgangspunt voor het onderzoek een centrale omgeving (in tegenstelling tot een gedistribueerde omgeving) waarin geen openbare mappen bestaan, en waarin de mailboxen geen aparte archiefmailbox hebben.

3.10. Verwerking informatieverzoeken

De verwerking van informatieverzoeken en de doorzoekbaarheid van mailboxen is onderdeel van fase 1b.

3.11. Het recht op rectificatie van gegevens uit de AVG

Artikel 16 van de AVG geeft betrokkenen (ambtenaren, burgers) het recht op rectificatie van hun persoonsgegevens. Voor fase 1a volgt hieruit geen eis aan de technische invulling; mogelijk is dat in fase 1b wel het geval.

4. Veiligstellen

4.1. Wat is het veiligstellen van e-mails?

Het veiligstellen van een e-mail betekent dat gedurende een vastgestelde periode de oorspronkelijke e-mail niet kan worden vernietigd.[11]

Technisch is het mogelijk een reeds ontvangen/verzonden oorspronkelijke e-mail nog aan te passen. Als die technische mogelijkheid niet kan worden uitgeschakeld, dient in elk geval de oorspronkelijke mail behouden te blijven en te worden bijgehouden wat er door wie wanneer is gewijzigd. Het behouden van het origineel, terwijl het ook mag worden aangepast lijkt tegenstrijdig, maar in de praktijk zal dat waarschijnlijk betekenen dat een exemplaar van het origineel bewaard blijft, terwijl een kopie mag worden aangepast.

4.2. Moment van veiligstellen

E-mail wordt tien weken na ontvangst/verzending veiliggesteld. In de praktijk is het misschien technisch niet mogelijk om dit op de seconde nauwkeurig tien weken na ontvangst/verzending van de e-mail te doen. Het veiligstellen mag dan ook batchgewijs zo snel mogelijk na afloop van de tienwekentermijn. Het moment van veiligstellen moet wel duidelijk zijn voor de eindgebruiker en eenduidig kunnen worden gecommuniceerd. Het moet voor de eindgebruiker herkenbaar zijn wanneer een e-mail wel of niet veiliggesteld is.

4.3. Welke items worden veiliggesteld?

Naast e-mails, worden ook bijvoorbeeld agendaverzoeken en contactpersonen opgeslagen in de mailbox van een eindgebruiker. Volgens de *Handreiking* moeten in ieder geval de e-mailberichten en bijbehorende bijlagen worden veiliggesteld. Bij het onderzoek hoeft echter geen beperking te worden aangebracht in de items in de Exchange-omgeving die mogen worden veiliggesteld, als daarmee gemakkelijker een technische oplossingsrichting kan worden gevonden. Dat betekent dat ook technische oplossingen mogen worden onderzocht die álle soorten items veiligstellen.

4.4. Veiliggestelde e-mail toch uitzonderen van veiligstellen, of toch vernietigen vóór de tienjaarstermijn

De eindgebruiker kan een e-mailbericht uitzonderen van veiligstellen door het te vernietigen, of door het als privé aan te merken (zie het volgende hoofdstuk). Dit kan alleen binnen de eerste tien weken na ontvangst/verzending van een e-mail. Als uitzondering op die hoofdregel moet het onder voorwaarden mogelijk zijn om ook ná die tien weken een

[11] In de *Handreiking* staat in de toelichting (paragraaf 3) dat e-mail-berichten in de map *Verwijderde items* niet worden veiliggesteld. Dat wordt geïnterpreteerd als een toelichting die van toepassing is op ander soort technische oplossing dan degene die nu wordt onderzocht. Het is toegestaan dat een gebruiker veiliggestelde e-mail door verwijdering (zie begrippenkader) uit zijn zicht kan plaatsen, of bijvoorbeeld in een map *Verwijderde items*, zolang het oorspronkelijke e-mailbericht kan worden teruggehaald, bijvoorbeeld bij een informatieverzoek.

e-mailbericht alsnog uit te zonderen van veiligstellen.[12] Enkele situaties waarin dit wenselijk is, zijn in de *Handreiking* benoemd: een verzoek tot vernietiging op grond van de AVG of een wettelijke vernietigingstermijn korter dan tien jaar. Ook willen eindgebruikers na langdurige afwezigheid alsnog niet-relevante e-mails (waaronder privé-berichten) kunnen uitzonderen van veiligstellen.

Het moet onmogelijk zijn voor de eindgebruiker zelf om een veiliggestelde e-mail na de tienwekentermijn alsnog te vernietigen, of als privé aan te merken. Het moet echter wel mogelijk zijn dat de zorgdrager aan de ICT-leverancier een opdracht geeft om een veiliggestelde e-mail na de tienwekentermijn alsnog te vernietigen, of als privé aan te merken. De zorgdrager of zijn gemandateerde mag een dergelijke opdracht geven. Ook wordt onderzocht of het mogelijk dat de zorgdrager of zijn gemandateerde zelf in het systeem de technische vernietigingsactie uitvoert.

In fase 1a wordt de mogelijkheid om veiliggestelde e-mails alsnog te vernietigen onderzocht. De mogelijkheid om veiliggestelde e-mails alsnog als privé aan te merken, wordt in fase 1b onderzocht. Ook de verklaring van vernietiging, die na vernietiging moet worden opgesteld, wordt in fase 1b onderzocht. De inhoud en detailniveau van die verklaring worden dan ook later besproken. Er gelden wat dat betreft geen randvoorwaarden aan de te onderzoeken technische oplossingsrichtingen.

[12] De omgekeerde situatie – een e-mail is als privé aangemerkt, maar moet na de tienwekentermijn toch worden veiliggesteld – staat beschreven in het volgende hoofdstuk.

5. Uitzonderen van veiligstellen

5.1. Hoe werkt het uitzonderen van veiligstellen?

Tien weken na ontvangst/verzending van een e-mail wordt deze automatisch voor tien jaar veiliggesteld. De eindgebruiker krijgt in de eerste tien weken na het ontvangen/verzenden van de e-mail de mogelijkheid om deze uit te zonderen van veiligstellen. Dat kan op twee manieren: (1) door de e-mail te verwijderen en (2) door de e-mail aan te merken als privé.

5.2. Uitzonderen door verwijderen

In de eerste tien weken na ontvangst/verzending van de e-mail, kan de eindgebruiker de e-mail verwijderen. De verwijderde e-mail is daarna nog enige tijd terug te halen, voor het geval de eindgebruiker de e-mail abusievelijk heeft verwijderd. Daarna wordt de e-mail technisch vernietigd, wat betekent dat de inhoud van de e-mail niet meer kan worden gereconstrueerd. Zie daarvoor ook de uitgebreidere toelichting in het begrippenkader (hoofdstuk 2).

Binnen de tienwekentermijn moet een (abusievelijk) verwijderde e-mail nog kunnen worden teruggehaald, zodat de verwijdering ongedaan gemaakt wordt. De verwijderde e-mail mag dus pas na afloop van de tienwekentermijn technisch worden vernietigd. Die technische vernietiging mag onmiddellijk na afloop van die tienwekentermijn plaatsvinden. Het heeft echter de voorkeur als een verwijderd bericht ook na de tienwekentermijn nog een korte tijd behouden blijft, en pas na die korte tijd technisch wordt vernietigd. Dan is het namelijk mogelijk om binnen die korte tijd na afloop van de tienwekentermijn een (abusievelijk) verwijderde e-mail nog terug te halen. Die korte tijd kan nader worden bepaald en ligt in de orde van grootte van een paar weken, zodat die korte tijd in verhouding staat tot de tienwekentermijn.

Na afloop van de tienwekentermijn is de e-mail veiliggesteld. Het mag technisch nog wel mogelijk zijn dat een eindgebruiker een veiliggestelde e-mail verwijdert, dus in de map *Verwijderde items* plaatst. Het mag technisch ook mogelijk zijn dat de e-mail (via de map *Deletions*) in de map *Purges*[13] terecht komt, en daarmee buiten het zicht van de eindgebruiker is geplaatst. Het moet echter technisch onmogelijk zijn dat de veiliggestelde e-mail technisch wordt vernietigd.

5.3. Uitzonderen door aanmerken als privé

Een eindgebruiker kan een e-mail binnen tien weken na ontvangst/verzending aanmerken als privé. Dit kan op verschillende manieren, bijvoorbeeld door een e-mail in een mapje 'Privé' te plaatsen, of door een e-mail een label/kenmerk te geven dat daar inhoudelijk mee overeenkomt. Deze functionaliteit is bedoeld om het mogelijk te maken dat niet-relevante e-mail wordt uitgezonderd van veiligstellen.

[13] Zie voor een (grafische) toelichting op deze mappen het begrippenkader in hoofdstuk 2.

Bij voorkeur kunnen e-mailberichten die als privé zijn aangemerkt, op elk moment (ook na de tienwekentermijn) door de eindgebruiker worden verwijderd, waarna ze (korte tijd later) technisch worden vernietigd.

5.4. Uitgezonderde e-mails toch veiligstellen

De uitgezonderde e-mails kunnen alsnog worden veiliggesteld, zowel binnen als na afloop van de tienwekentermijn. De eindgebruiker kan dit zelf doen, zonder tussenkomst van de zorgdrager. Als een uitgezonderde e-mail alsnog wordt veiliggesteld, verandert daarmee het moment van ontvangst/verzending van de e-mail niet.

6. Vernietigen

6.1. Het proces van vernietigen

E-mail die is veiliggesteld, wordt op een zeker moment vernietigd: de e-mail doorloopt het proces van vernietigen, waarvan het daadwerkelijk wissen (technisch vernietigen) van de e-mail een belangrijk onderdeel is. Conform de Archiefwet omvat het proces meer elementen, bijvoorbeeld het opmaken van een verklaring van vernietiging.[14]

Voor alle veiliggestelde e-mails zal die vernietiging plaatsvinden tien jaar na ontvangst/verzending van de e-mail (zie paragraaf 6.3), tenzij een uitzondering van toepassing is. Die uitzondering kan zijn dat het bericht al eerder wordt vernietigd (paragraaf 6.4), of wordt overgedragen aan het Nationaal Archief (paragraaf 6.5 en 6.6).

E-mails die zijn uitgezonderd van veiligstellen, doorlopen niet het proces van vernietigen. Als het uitzonderen van veiligstellen plaatsvond door het bericht te verwijderen, is het bericht al kort na de tienwekentermijn technisch vernietigd (zie paragraaf 5.2). Voor de volledigheid staat in paragraaf 6.2 ook hoe wordt omgegaan met het technisch vernietigen van berichten die als privé zijn aangemerkt.

6.2. Wat wordt vernietigd?

Zoals hierboven vermeld, heeft het proces van vernietigen betrekking op e-mails die zijn veiliggesteld in de Exchange-omgeving. Dat alle veiliggestelde e-mail tien jaar na ontvangst/verzending wordt vernietigd, betekent dus ook dat e-mails in de Inbox, Verzonden items of andere zelfgemaakte mappen worden vernietigd.[15]

E-mails die zijn uitgezonderd van veiligstellen door ze als privé aan te merken, worden niet vernietigd, omdat ze niet zijn veiliggesteld. Niettemin mogen de uitgezonderde items bij gedeactiveerde accounts (vaak na uitdiensttreding/overplaatsing) tien jaar na deactivatie technisch worden vernietigd. Dat voorkomt dat de uitgezonderde items ongelimiteerd bewaard moeten blijven, terwijl de betreffende eindgebruiker (zonder account) geen toegang meer heeft tot die gegevens.

Het vernietigen ziet op de e-mails in de Exchange-omgeving. Als buiten die omgeving een back-up wordt gemaakt om gegevens bij een calamiteit weer terug te kunnen zetten, dienen evenwel ook de e-mails in de back-up technisch te worden vernietigd. De back-ups dienen een ander doel en hebben hun eigen doorlooptijd, maar de technische vernietiging dient binnen een redelijke termijn plaats te vinden.

6.3. Moment van vernietigen

Het moment van vernietigen ligt niet per definitie direct/exact na afloop van de bewaartermijn van tien jaar. Het vernietigen zelf kost immers ook tijd. Het heeft de voorkeur dat de vernietiging niet te lang na afloop van

[14] De verklaring van vernietiging wordt in fase 1b onderzocht, zie paragraaf 4.4.
[15] Of de zorgdrager vóór vernietiging nog een signaal krijgt, kan in fase 1b worden besproken.

de tienjaarstermijn plaatsvindt. Dat kan bijvoorbeeld in maandelijkse batches. Dit betekent mogelijk dat er bijvoorbeeld drie tot zes maanden vóór het aflopen van de bewaartermijn een beoordeling door de zorgdrager moet plaatsvinden. Daarover moeten nog procedurele afspraken worden gemaakt. Dat leidt op dit moment echter niet tot aanvullende randvoorwaarden aan de technische oplossingsrichtingen.

Het is de wens om de vernietiging van een e-mail te kunnen blokkeren, bijvoorbeeld als die e-mail een rol speelt bij een rechtszaak. Dat zal in opdracht van de zorgdrager zijn. De eindgebruiker heeft namelijk geen zeggenschap over veiliggestelde e-mails. Ook wordt onderzocht of de zorgdrager of zijn gemandateerde zelf in het systeem de vernietiging kan blokkeren.

6.4. Eerdere vernietiging dan na tien jaar

E-mail met een bij wet gestelde vernietigingstermijn korter dan tien jaar wordt na verstrijken van deze termijn vernietigd. Die kortere vernietigingstermijn kan van tevoren vaststaan, maar is in sommige gevallen onbekend. In de *Handreiking* worden als voorbeeld vernietigingstermijnen genoemd die samenhangen met het moment van rechterlijke uitspraak of overlijden van een persoon.
Om de vernietiging van veiliggestelde e-mails vóór het verstrijken van de tienjaarstermijn mogelijk te maken, wordt aangesloten bij de functionaliteit die in paragraaf 4.4 is beschreven: de zorgdrager of zijn gemandateerde kan de ICT-leverancier opdracht geven om een veiliggestelde e-mail na de tienwekentermijn alsnog te vernietigen.

In aanvulling daarop wordt in fase 1b onderzocht of de zorgdrager of zijn gemandateerde de mogelijkheid kan krijgen om zelf in het systeem de selectie van te vernietigen e-mails te maken en de technische vernietigingsactie uit te voeren.

6.5. Hotspots

Er moet een selectie op basis van zoektermen gemaakt kunnen worden uit alle e-mails binnen (een selectie van) een departement, waarna die e-mails ofwel als collectie apart worden gezet (bijvoorbeeld in een PST-bestand), ofwel alvast worden overgebracht naar het Nationaal Archief. Zo kunnen e-mails over een bepaald onderwerp of gebeurtenis worden veiliggesteld (‘hotspots’, zie ook paragraaf 2.6). Dat is een van de invullingen van de opmerking in de *Handreiking* dat e-mail van niet-sleutelfunctionarissen in bepaalde gevallen uitgezonderd kan worden van vernietiging en permanent bewaard kan worden. Het uitzonderen van vernietiging van e-mails van niet-sleutelfunctionarissen (inclusief hotspot-functionaliteit) wordt in fase 1b onderzocht.

6.6. Samenloop van vernietigen en overdragen

Als het e-mail betreft die wordt overgedragen aan het Nationaal Archief, dan vindt de technische vernietiging in de e-mailomgeving van de ICT-leverancier pas plaats na succesvolle overdracht aan het Nationaal Archief. Dit wordt in fase 1b onderzocht.

7. Bijlage 1. Deelnemerslijst voorbereidende sessies

De volgende mensen hebben deelgenomen aan één of meerdere overleggen (deels alleen binnen SSC-ICT) waarin dit document is voorbereid.

Naam	Organisatie	Rol in project E-mail bewaren
(geanonimiseerd)	RDDI	Programmadirecteur
(geanonimiseerd)	RDDI	Projectleider E-mailarchivering
(geanonimiseerd)	RDDI	Projectsecretaris E-mailarchivering
(geanonimiseerd)	RDDI	DUTO-adviseur, vanuit Nationaal Archief
(geanonimiseerd)	RDDI	Projectadviseur, vanuit Nationaal Archief
(geanonimiseerd)	RDDI	Projectadviseur, vanuit JenV
(geanonimiseerd)	RDDI	Projectadviseur, vanuit VWS
(geanonimiseerd)	SSC-ICT	Servicedomeinadviseur Rijkswerkomgeving
(geanonimiseerd)	SSC-ICT	Projectleider SSC-ICT
(geanonimiseerd)	SSC-ICT	Domeinarchitect Applicaties
(geanonimiseerd)	SSC-ICT	Domeinarchitect Persoonlijke WerkOmgeving
(geanonimiseerd)	SSC-ICT	Privacy officer
(geanonimiseerd)	SSC-ICT	Security officer
(geanonimiseerd)	SSC-ICT	Technisch Architect Exchange-omgeving
(geanonimiseerd)	SSC-ICT	Beheerder Exchange JenV

Bijlage 3. Eisen en wensen uit de *Interpretatie*

In de *Interpretatie* zijn de eisen en wensen voor drie van de vier hoofdfunctionaliteiten beschreven (zie paragraaf 3.1): *Veiligstellen*, *Uitzonderen van veiligstellen* en *Vernietigen*. SSC-ICT heeft uit de *Interpretatie* eenentwintig eisen en wensen geïdentificeerd. SSC-ICT heeft een inschatting gemaakt van de kans dat ofwel de eis technisch onuitvoerbaar is, ofwel dat aan de oplossing grote risico's of nadelen kleven. Die inschatting is gemaakt op basis van de voorlopige inzichten bij SSC-ICT die mede door de gesprekken met de experts van Microsoft zijn ontstaan. Negen eisen hadden een grote kans daarop en zijn in fase 1a onderzocht.

In deze bijlage zijn alle 21 eisen en wensen opgesomd. Daarbij is aangegeven wat de vindplaats in de *Interpretatie* is, bij welke hoofdfunctionaliteit de eis hoort, en of de kans klein/medium/groot was ingeschat dat ofwel de eis technisch onuitvoerbaar is, ofwel dat aan de oplossing grote risico's of nadelen kleven.

Om verwarring met de negen onderzochte eisen (genummerd van 1 tot 9) te voorkomen, zijn de eisen met letters genummerd. De zijn gesorteerd op de volgorde van vermelding in de *Interpretatie*. Dat voor de negen onderzochte eisen een andere volgorde dan dat ze in hoofdstuk 3 zijn gepresenteerd.

Eis A. Herkenbaarheid voor de eindgebruikers
"Het is in het algemeen wenselijk[60] als de hele werkwijze voor de eindgebruiker zo intuïtief mogelijk werkt en er voor de eindgebruikers zo min mogelijk verandert aan de huidige interfaces (Outlook en BlackBerry) en werkwijze. De eindgebruiker moet bovendien op een eenvoudige manier het onderscheid kunnen herkennen tussen de volgende drie categorieën e-mails: (1) veiliggestelde e-mails, (2) e-mails die zijn uitgezonderd van veiligstellen en (3) e-mails die niet zijn veiliggesteld én niet zijn uitgezonderd. In deze derde categorie zitten de e-mails die nog geen tien weken oud zijn en dus nog niet zijn veiliggesteld, terwijl deze e-mails ook (nog) niet door de eindgebruiker zijn uitgezonderd van veiligstellen."
Vindplaats: paragraaf 3.2 van de *Interpretatie*.
Hoofdfunctionaliteit: geen/algemeen
Kans: medium
Onderzocht: nee

[60] Deze eis is eigenlijk tweeledig. Een wens (de eerste zin) en een eis (de rest van de alinea).

Eis B. De werkwijze moet per mailbox aan en uit kunnen worden geschakeld
"Het moet technisch mogelijk zijn om in opdracht van de zorgdrager (functionele) mailboxen uit te zonderen van de toepassing van de werkwijze van de *Handreiking*. Dit kan bijvoorbeeld gewenst zijn voor de (functionele) mailbox van een integriteitscoördinator of een bedrijfsarts, maar maakt het bovendien mogelijk om de werkwijze binnen een departement gefaseerd in te voeren."
Vindplaats: paragraaf 3.4 van de *Interpretatie*.
Hoofdfunctionaliteit: geen/algemeen
Kans: klein
Onderzocht: nee

Eis C. Werkwijze geldt ook voor functionele postbussen
"Voor dit onderzoek wordt geen onderscheid gemaakt tussen een functionele postbus en een reguliere mailbox van een eindgebruiker. Dat betekent bijvoorbeeld ook dat de eindgebruikers die toegang hebben tot een functionele postbus, op dezelfde manier e-mails kunnen uitzonderen van veiligstellen."
Vindplaats: paragraaf 3.5 van de *Interpretatie*.
Hoofdfunctionaliteit: geen/algemeen
Kans: klein
Onderzocht: nee

Eis D. Werkwijze blijft gelden voor inactieve mailboxen
"De werkwijze van de *Handreiking* moet ook voor inactieve mailboxen gelden."
Vindplaats: paragraaf 3.6 van de *Interpretatie*.
Hoofdfunctionaliteit: geen/algemeen
Kans: klein
Onderzocht: nee

Eis E. Oorspronkelijke e-mail niet vernietigen
"Het veiligstellen van een e-mail betekent dat gedurende een vastgestelde periode de oorspronkelijke e-mail niet kan worden vernietigd."
Vindplaats: paragraaf 4.1 van de *Interpretatie*.
Hoofdfunctionaliteit: veiligstellen
Kans: klein
Onderzocht: nee

Eis F. Wijzigingen in e-mails bijhouden
"Technisch is het mogelijk een reeds ontvangen/verzonden oorspronkelijke e-mail nog aan te passen. Als die technische mogelijkheid niet kan worden uitgeschakeld, dient in elk geval de oorspronkelijke mail behouden te blijven en te worden bijgehouden wat er door wie wanneer is gewijzigd."
Vindplaats: paragraaf 4.1 van de *Interpretatie*.
Hoofdfunctionaliteit: veiligstellen
Kans: klein
Onderzocht: nee

Eis G. E-mail wordt tien weken na ontvangst/verzending veiliggesteld
"E-mail wordt tien weken na ontvangst/verzending veiliggesteld. In de praktijk is het misschien technisch niet mogelijk om dit op de seconde nauwkeurig tien weken na ontvangst/verzending van de e-mail te doen. Het veiligstellen mag dan ook batchgewijs zo snel mogelijk na afloop van de tienwekentermijn."
Vindplaats: paragraaf 4.2 van de Interpretatie.
Hoofdfunctionaliteit: veiligstellen
Kans: groot
Onderzocht: ja, als eis 1

Eis H. Andere items dan e-mails optioneel veiligstellen
"Naast e-mails, worden ook bijvoorbeeld agendaverzoeken en contactpersonen opgeslagen in de mailbox van een eindgebruiker. Volgens de *Handreiking* moeten in ieder geval de e-mailberichten en bijbehorende bijlagen worden veiliggesteld. Bij het onderzoek hoeft echter geen beperking te worden aangebracht in de items in de Exchange-omgeving die mogen worden veiliggesteld, als daarmee gemakkelijker een technische oplossingsrichting kan worden gevonden."
Vindplaats: paragraaf 4.3 van de *Interpretatie*.
Hoofdfunctionaliteit: veiligstellen
Kans: klein
Onderzocht: nee

Eis I. Eindgebruiker kan na tien weken e-mail niet meer vernietigen
"Het moet onmogelijk zijn voor de eindgebruiker zelf om een veiliggestelde e-mail na de tienwekentermijn alsnog te vernietigen"
Vindplaats: paragraaf 4.4 van de *Interpretatie*.
Hoofdfunctionaliteit: veiligstellen
Kans: klein
Onderzocht: nee

Eis J. Eindgebruiker kan na tien weken e-mail niet meer als privé aanmerken
"Het moet onmogelijk zijn voor de eindgebruiker zelf om een veiliggestelde e-mail na de tienwekentermijn alsnog als privé aan te merken."
Vindplaats: paragraaf 4.4 van de *Interpretatie*.
Hoofdfunctionaliteit: veiligstellen
Kans: groot
Onderzocht: ja, als eis 7

Eis K. Zorgdrager kan na tien weken e-mail nog wel vernietigen of als privé aanmerken
"Het moet echter wel mogelijk zijn dat de zorgdrager aan de ICT-leverancier een opdracht geeft om een veiliggestelde e-mail na de tienwekentermijn alsnog te vernietigen, of als privé aan te merken."
Vindplaats: paragraaf 4.4 van de *Interpretatie*.

Hoofdfunctionaliteit: veiligstellen
Kans: groot
Onderzocht: ja, als eis 8

Eis L. Eindgebruiker kan e-mail vernietigen binnen tien weken na ontvangst/verzending
"In de eerste tien weken na ontvangst/verzending van de e-mail, kan de eindgebruiker de e-mail verwijderen. De verwijderde e-mail is daarna nog enige tijd terug te halen, voor het geval de eindgebruiker de e-mail abusievelijk heeft verwijderd. Daarna wordt de e-mail technisch vernietigd, wat betekent dat de inhoud van de e-mail niet meer kan worden gereconstrueerd."
Vindplaats: paragraaf 5.2 van de *Interpretatie*.
Hoofdfunctionaliteit: uitzonderen
Kans: groot
Onderzocht: ja, als eis 3

Eis M. Terughalen verwijderde e-mail binnen tienwekentermijn
"Binnen de tienwekentermijn moet een (abusievelijk) verwijderde e-mail nog kunnen worden teruggehaald, zodat de verwijdering ongedaan gemaakt wordt. De verwijderde e-mail mag dus pas na afloop van de tienwekentermijn technisch worden vernietigd."
Vindplaats: paragraaf 5.2 van de *Interpretatie*.
Hoofdfunctionaliteit: uitzonderen
Kans: groot
Onderzocht: ja, als eis 4

Eis N. Terughalen verwijderde e-mail nog korte tijd na tienwekentermijn mogelijk
"Die technische vernietiging mag onmiddellijk na afloop van die tienwekentermijn plaatsvinden. Het heeft echter de voorkeur als een verwijderd bericht ook na de tienwekentermijn nog een korte tijd behouden blijft, en pas na die korte tijd technisch wordt vernietigd. Dan is het namelijk mogelijk om binnen die korte tijd na afloop van de tienwekentermijn een (abusievelijk) verwijderde e-mail nog terug te halen. Die korte tijd kan nader worden bepaald en ligt in de orde van grootte van een paar weken, zodat die korte tijd in verhouding staat tot de tienwekentermijn."
Vindplaats: paragraaf 5.2 van de *Interpretatie*.
Hoofdfunctionaliteit: uitzonderen
Kans: groot
Onderzocht: ja, als eis 5

Eis O. Eindgebruiker kan e-mail binnen tien weken na ontvangst/verzending aanmerken als privé
"Een eindgebruiker kan een e-mail binnen tien weken na ontvangst/verzending aanmerken als privé. Deze functionaliteit is bedoeld om het mogelijk te maken dat niet-relevante e-mail wordt uitgezonderd van veiligstellen."
Vindplaats: paragraaf 5.3 van de *Interpretatie*.

Hoofdfunctionaliteit: uitzonderen
Kans: groot
Onderzocht: ja, als eis 6

Eis P. Uitgezonderde e-mail alsnog veiligstellen
"De uitgezonderde e-mails kunnen alsnog worden veiliggesteld, zowel binnen als na afloop van de tienwekentermijn. De eindgebruiker kan dit zelf doen, zonder tussenkomst van de zorgdrager."
Vindplaats: paragraaf 5.4 van de *Interpretatie*.
Hoofdfunctionaliteit: uitzonderen
Kans: medium
Onderzocht: nee

Eis Q. Veiliggestelde e-mails na tien jaar vernietigen
"E-mail die is veiliggesteld, wordt op een zeker moment vernietigd. Voor alle veiliggestelde e-mails zal die vernietiging plaatsvinden tien jaar na ontvangst/verzending van de e-mail. Het moment van vernietigen ligt niet per definitie direct/exact na afloop van de bewaartermijn van tien jaar. Het vernietigen zelf kost immers ook tijd. Het heeft de voorkeur dat de vernietiging niet te lang na afloop van de tienjaarstermijn plaatsvindt. Dat kan bijvoorbeeld in maandelijkse batches."
Vindplaats: paragraaf 6.1 en 6.3 van de *Interpretatie*.
Hoofdfunctionaliteit: vernietigen
Kans: groot
Onderzocht: ja, als eis 2

Eis R. Als privé aangemerkte e-mails worden niet na tien jaar automatisch vernietigd
"E-mails die zijn uitgezonderd van veiligstellen door ze als privé aan te merken, worden niet vernietigd, omdat ze niet zijn veiliggesteld."
Vindplaats: paragraaf 6.2 van de *Interpretatie*.
Hoofdfunctionaliteit: vernietigen
Kans: groot
Onderzocht: ja, als eis 9

Eis S. Als privé aangemerkte e-mails van gedeactiveerde accounts vernietigen na tien jaar
"Niettemin mogen de uitgezonderde items bij gedeactiveerde accounts (vaak na uitdiensttreding/overplaatsing) tien jaar na deactivatie technisch worden vernietigd."
Vindplaats: paragraaf 6.2 van de *Interpretatie*.
Hoofdfunctionaliteit: vernietigen
Kans: klein
Onderzocht: nee

Eis T. Vernietigen e-mails uit back-ups
"Het vernietigen ziet op de e-mails in de Exchange-omgeving. Als buiten die omgeving een back-up wordt gemaakt om gegevens bij een calamiteit weer terug te kunnen zetten, dienen evenwel ook de e-mails in de back-up technisch te worden vernietigd."

Vindplaats: paragraaf 6.2 van de *Interpretatie*.
Hoofdfunctionaliteit: vernietigen
Kans: klein
Onderzocht: nee

Eis U. Blokkeren van de vernietiging van e-mails voor een individuele mailbox
"Het is de wens om de vernietiging van een e-mail te kunnen blokkeren, bijvoorbeeld als die e-mail een rol speelt bij een rechtszaak."
Vindplaats: paragraaf 6.3 van de *Interpretatie*.
Hoofdfunctionaliteit: vernietigen
Kans: medium
Onderzocht: nee

Bijlage 4. Betrokkenen bij het onderzoek

Aan de begeleidingsgroep vanuit de opdrachtgever hebben de volgende personen deelgenomen.

Naam	**Rol in RDDI-project E-mailarchivering**
(geanonimiseerd)	Projectleider E-mailarchivering
(geanonimiseerd)	Projectadviseur E-mailarchivering
(geanonimiseerd)	ICT-adviseur RDDI
(geanonimiseerd)	DUTO-adviseur, vanuit Nationaal Archief
(geanonimiseerd)	Projectadviseur, vanuit Nationaal Archief
(geanonimiseerd)	Projectadviseur, vanuit JenV
(geanonimiseerd)	Projectadviseur, vanuit VWS

Vanuit SSC-ICT hebben de volgende personen meegewerkt aan het onderzoek.

Naam	**Rol**
(geanonimiseerd)	Servicedomeinadviseur Rijkswerkomgeving
(geanonimiseerd)	Projectleider SSC-ICT
(geanonimiseerd)	Domeinarchitect Applicaties
(geanonimiseerd)	Domeinarchitect Persoonlijke WerkOmgeving
(geanonimiseerd)	Privacy officer
(geanonimiseerd)	Security officer
(geanonimiseerd)	Technisch Architect Exchange-omgeving
(geanonimiseerd)	Beheerder Exchange JenV

Vanuit Microsoft hebben de volgende personen meegewerkt aan het onderzoek.

Naam	**Rol**
(geanonimiseerd)	Digital Architect
(geanonimiseerd)	Senior Consultant Exchange
(geanonimiseerd)	Senior Consultant Exchange