Tips voor behandeling van het onderwerp E-mail-archivering door (departementale) ondernemingsraden.

Aanleiding
Binnen de Rijksoverheid was het slecht gesteld met de naleving van de wettelijke eisen rondom archiefvorming en naspeurbaarheid van besluiten.

Het merendeel (80%) van de beslisinformatie van de rijksdienst wordt uitsluitend in het immer groeiende e-mail-verkeer vastgelegd. Dat zijn ongeveer 100.000 nieuwe e-mails per uur.
Het Rijksbrede traject Duurzame Digitale Informatiehuishouding (RDDI) formuleerde een oplossing in de vorm van een **Handreiking 'Bewaren van E-mail Rijksoverheid'**. Deze handreiking is besproken in de werkgroep privacy van de GOR Rijk maar is nooit formeel op de bestuurstafel behandeld.
In 2021 is aan de Tweede Kamer toegezegd dat de kerndepartementen eind 2021 volgens deze methode gaan werken. Die termijn bleek niet haalbaar, onder meer vanwege technische problemen. De (kern)departementen hebben toen een jaar uitstel gekregen (eind 2022 conform de opzet van de Handreiking).

Addertje onder het gras is dat in december 2021 de Interdepartementale Commissie Bedrijfsvoering Rijk (ICBR) heeft besloten per omgaande alle e-mails van Rijksambtenaren veilig te stellen. Dus inclusief alle privacygevoelige mails. Dat kunnen onder andere mails zijn die persoonsgegevens bevatten zoals sollicitatiecorrespondentie, verzuiminformatie, mails over medische onderzoeken etc. Alle mails, nu dus ook de privacygevoelige mails, zijn op basis van de WOB/WOO doorzoekbaar. Uiteraard indien daartoe aanleiding is en de gewone zoek/opvraag-procedure te weinig effect sorteert.

Het programma Open Op Orde, waar e-mail archivering nu onder valt heeft, op initiatief van de werkgroep IV-ICT van de GOR Rijk, in de ICBR aandacht gevraagd voor het betrekken van de (departementale) ondernemingsraden bij de implementatie van de handreiking 'Bewaren van E-mail verkeer Rijksoverheid' in hun departement.

In ideale vorm zou die betrokkenheid en formele afhandeling de volgende punten omvatten:
1) De technische en organisatorische voorzieningen om de toepassing van de handreiking 'Bewaren van E-mail Rijksoverheid' binnen het departement op passende wijze in te voeren;
2) Deze voorzieningen te laten beoordelen op risico's voor de privacy: uitvoeren van een Data Protection Impact Assessment (DPIA) met daarbij speciale aandacht voor communicatie naar de medewerkers. Zo zouden medewerkers bewust gemaakt moeten worden en zouden instructies gegeven moeten worden. Ook zouden voorzieningen aangeboden moeten worden en monitoring moeten plaatsvinden op de naleving.
3) Het door de departementen op te stellen 'Doorzoekprotocol' (de implementatie van een 'Zoek en vind' functionaliteit) zou afgestemd moeten worden met de (D)OR als zijnde een regeling voor de verwerking van persoonsgegevens binnen de onderneming. Uiteraard zijn het laten beoordelen van de privacy-risico's (d.m.v. een DPIA) en het in kaart brengen van risico's op het gebied van Artificial Intelligence (AI), bijvoorbeeld door het houden van een Impact Assessment Mensenrechten en Algoritmes -IAMA-) onderdeel van de afstemming. Wellicht is deze laatste (IAMA) op de softwarekeuze een generieke taak voor de Privacy Adviseur Rijk (PAR) en de GroepsOndernemingsRaad Rijk (GOR Rijk).

Tips voor de departementale en lokale ondernemingsraden
Hoewel e-mail archivering Rijksbreed is afgesproken, is de implementatie en inbedding in de onderdelen en ZBO's een departementale aangelegenheid.

Vandaar deze tips voor verdere behandeling bij de medezeggenschap van de departementen en Rijksonderdelen.
1) Bespreek E-mail-archivering met de bestuurder. Bijvoorbeeld in een artikel 24 overleg; benoem daarbij de snelheidsverschillen in het departement: de toezegging is operationeel in 2023 voor kerndepartement en in 2026 voor de overige dienstonderdelen.
2) Stel daarbij dat de technisch organisatorische uitwerking binnen het departement een regeling is omtrent het verwerken van en de bescherming van persoonsgegevens van de in de onderneming werkzame personen (WOR Artikel 27 k).

3) Stel daarbij dat een departementale of onderdeel specifieke uitwerking een specifieke beoordeling van de privacy vraagt. Het vereist dus een eigen DPIA of andere vorm van privacy beoordeling door een privacy professional.
4) Maak afspraken over eventueel technisch overleg met de stakeholder(s) en partijen die betrokken zijn bij de departementale uitwerking voor het volgen van de technische aspecten en het maatwerk dat daaruit ontstaat. Denk hierbij aan de CIO, de projectmanager/-leider Open Op Orde, de projectleider IV, de privacy officer, en anderen.
5) Maak tenminste procesafspraken voor de volgende drie majeure onderwerpen:
    a. De omgang met reeds zeker gestelde E-mails:
    Deze kunnen tot 2026 of langer ongeschoond blijven. Indien toegang wordt verleend tot deze mails, verdient dat een classificatie als een apart instemmingsplichtig besluit: mag de WOO-adviseur op grond van "overeengekomen criteria" de ongeschoonde e-mails doorzoeken?
    b. Het Doorzoekprotocol:
    Dit regelt de bevoegdheden van de WOO-adviseurs en is eveneens een regeling voor het verwerken van alsmede de bescherming van persoonsgegevens van de in de onderneming werkzame personen (WOR Artikel 27k). Zet in op een aparte DPIA en IAMA omdat de zoek- en vind-software en de WOO-software AI-based technologie bevat.
    c. Het opschonen van e-mails vergt zowel bewustwording en vaardigheid als voldoende tijd:
    Draag zorg voor een gebalanceerde voorlichtingscampagne. Laat de bestuurder oploopjes en polls, Q&A's en hulplijnen organiseren (of organiseer dit samen met de bestuurder). Bespreek de werkdruk die mogelijk voortvloeit uit inhaalslagen en het dagelijks opschonen.
6) Blijf de vinger aan de pols houden, maak afspraken over (onafhankelijke) evaluaties en hoe stakeholders en verantwoordelijken het proces verder kunnen verbeteren.

Leestip:
Implementatie e-mailarchivering | Rijksprogramma voor Duurzaam Digitale Informatiehuishouding