# Verslag: bespreken memo SG Zoeken en vinden

Datum: 28-5-2020
Deelnemers: (10)(2e) (10)(2e) (10)(2e) (Projectleider Corona Archivering), (10)(2e) (10)(2e) (Beveiligingsambtenaar), (10)(2e) (10)(2e) (WOB coördinaten WJZ), (10)(2e) (10)(2e) (FGH VWS), (10)(2e) (CISO en Privacy Officer VWS kerndepartement), (10)(2e) (Notulen)
Afwezig: (10)(2e)

Context van het memo wordt door (10)(2e) (10)(2e) (10)(2e) en (10)(2e) (10)(2e) geschetst.
Projectopdracht project Corona Archivering is in het kort: Stel Corona gerelateerde informatie veilig. Welke informatie is er, waar staat de informatie en stel het veilig. Hier is een direct belang met WOB. Als je weet wat er is aan informatie en waar het staat, kun je WOB-verzoeken beantwoorden.

In het kader van het project gaan adviseurs van het project langs bij alle directies. Er wordt gevraagd of medewerkers binnen een directie met corona bezig zijn. Ook vragen zij toegang tot bronnen (zoals netwerkschijven, mailboxen) om onderzoek te doen. Dit geeft zeer veel bronnen en informatie. WOB verzoeken worden straks op eenzelfde wijze onderzocht.

Binnen VWS is software beschikbaar (Zoek en Vind van DocDirect). Deze software (nog in pilot fase) kan middels zoekvragen informatie vinden op netwerkschijven. Vanuit zowel het project Corona Archivering als de WOB, willen wij graag die software gebruiken om in te zetten binnen. Dan is er wel op hoog niveau toestemming nodig om toegang te krijgen tot de betreffende bronnen (netwerkschijven, mailboxen). Als die toestemming er is en de software kan worden ingezet, dan kunnen er informatiesets worden veiliggesteld en aan het WOB-traject worden gegeven ter beantwoording van de WOB-verzoeken.

Inmiddels zijn er ca. 50 WOB-verzoeken. Ca 10 zijn afkomstig van de pers, de rest is afkomstig van burgers. Tot nu toe zijn deze allemaal opgeschort. WOB-verzoeken vergen te veel tijd van de betrokken ambtenaren. In de Tweede Kamer zijn inmiddels vragen gesteld en moeten n.a.v. deze politieke druk nu WOB-verzoeken van de pers wel beantwoord worden. Wob traject start vanaf 2 juni. Wij mogen als project de medewerkers niet lastigvallen en de omvang van de datasets is zeer groot, daarom is software nodig om de deadlines van WOB-verzoeken te kunnen halen (of in ieder geval te in de buurt van de deadline te komen).

Daarom is de vraag gesteld door onze opdrachtgevers om hierover een memo op te stellen, waarin wordt uiteengezet wat er aan software nodig is en waarom. De SG heeft al akkoord gegeven over toegang tot o.a. mailboxen.

**Vragen n.a.v. context:**
(10)(2e) *(FG):* Goede onderbouwing is van groot belang. Die mist nu op diverse punten in het memo. De grondslag is niet uitgewerkt. Onderbouwing van grondslag met 'op basis van wetgeving' is te vaag, om in mailboxen van medewerkers te mogen zoeken. En over welke risico's hebben we het? Er is onvoldoende uitgewerkt hoe wordt omgegaan met bijvoorbeeld informatie die inhoudelijk raakt aan medisch beroepsgeheim en bijzondere persoonsgegevens. Zoek en Vind zoekt alleen op metagegevens wordt gesteld. Helder moet zijn of er ook wordt gezocht in de mail, in de bijlagen, etc. Grootste bezwaar zit voor (10)(2e) in de grondslag, maar is deze is mogelijk overkomelijk.

Overall t.a.v. het memo: De volgordelijkheid moet kloppen in het memo. Ineens komen IBabs en Topdesk voorbij.

(10)(2e) *(Beveiligingsambtenaar):* Ik kijk achteraf of reguliere regelgeving is gevolgd, en of de risico's anders bewust geaccepteerd zijn. Ik hoor nu dat er software wordt ingezet en die kijkt naar metagegevens. Maar geloven wij de leveranciers op hun blauwe ogen? Dat is niet goed genoeg in huidig klimaat (externe overheden/partijen hebben meer en meer interesse in ministeriële informatie). Wil je alles goed borgen, dan op AIVD niveau dichten. Anders moet je de risico's accepteren. Dat is een bevoegdheid van het lijnmanagement. Zorg dat de keuzes wel transparant worden gemaakt.

Tip: ga op bezoek bij BZK om hierover te praten. Daar veel kennis over WOB-verzoeken.

(10)(2e) *(CISO):* Het is niet duidelijk welke bronnen worden doorzocht door de software. Duidelijk moet zijn wat je gaat doorzoeken en welke scope je hanteert? Met de huidige opzet gaan we alle gemaakte regels over gegevensbeveiliging overtreden. Streng toegangsbeheer op bepaalde directieschijven kan niet simpelweg worden opzijgeschoven, ook niet door SG.
Met het oog op de toekomst zijn er ook risico's. Wat als we deze werkwijze als standaard gaan zien en directies het willen gaan inzetten voor toekomstige vragen? Hoe lang duurt de crisis? Dus hoelang is die toegang tot alle informatie wel niet nodig?

(10)(2e) Hierbij moeten we ook kijken naar de vraag 'Waarom zitten we in deze situatie?'. Dat komt, omdat gemaakt beleid rondom archivering niet wordt nageleefd. Informatie staat niet in de juiste archieven, waardoor het beantwoorden van een WOB-verzoek zeer complex wordt.

(10)(2e): Dat kun je zo niet gebruiken als onderbouwing. Je maakt probleem alleen maar groter.
Je wilt nu regels voorbijgaan, omdat je niet aan je initiële archiefverplichting voldoet. De gemiddelde medewerker weet waarschijnlijk ook niets van rubricering, waardoor er ook departementaal vertrouwelijk informatie op schijven kan staan. Doe je er dan wijs aan om voor een u-bocht te kiezen?

(10)(2e) Als je het werk met mensen gaat uitvoeren, dan verandert er niet zo veel. Die gaan mailboxen openen en mails lezen.

(10)(2e): Dat zijn dan wel VWS mensen die wij betrouwbaar achtten en je hebt dan een audit trail. Zijn er nu mensen betrokken geweest die kunnen aantonen dat die software niks doet dat het niet mag doen? Is het vastgesteld dat software veilig is? Anders moet je aan voorkant dat risico vastleggen.

**Privacy:**
(10)(2e): Het probleem is het doorzoeken van persoonlijke mailboxen. Wat is dan je onderbouwing voor doorzoeken van die mailboxen? Ik wil hier de afweging onderbouwd voorzien. Bijvoorbeeld: als medewerker ziek is en je hebt die gegevens nodig, dan mag je van AP de mailbox doorzoeken vanuit het belang van de doorgang van de werkprocessen. We zouden nu kunnen zeggen: WOB-verzoeken zijn van algemeen belang om vragen van media te beantwoorden. In het licht van belasting crisismedewerkers zouden we dan de afwezig kunnen maken om toch te gaan zoeken. Lees hiertoe de AP goed.

In het memo hoort ook te staan 'Een medewerker heeft wel/niet gelegenheid gekregen om privé mail weg te halen'. Dit moet een bekend risico zijn, dat al dan niet geaccepeteerd wordt

**Netwerkschijven:**
(10)(2e) : Wat is de scope en wat gaan we doorzoeken? Bijvoorbeeld IGJ, CCMO, ESST, WJZ. (opsporingszaken en gezondheid gegevens) kennen zware vertrouwelijkheden en beveiliging. Wat is de onderbouwing om beveiligingsschil te doorbreken? Zijn deze directies hierover tijdig geïnformeerd? Welke software wordt ingezet? Is die inpandig en welke waarborging geef je? Wie doet het werk? En bouw je bijvoorbeeld een 4-ogen principe in?

Advies: Doe een Privacy Impact Assesment en een Quickscan.

Voorstel: Doe de Quickscan. Schrijf vervolgens op hoe het proces gaat verlopen, wie er bij de informatie kan en welke risico's VWS dan loopt. Het overzicht van de risico's moeten in beeld zijn bij SG. Ook moet helder zijn over welke doelgroepen we het hebben. Welke medewerkers, welke dienstonderdelen (vertrouwelijkheden verschillen per directe/afdeling). Ben je betrokken bij corona? (10)(2e) de populatie in. Je mag directie niet doorzoeken als zij niet geïnformeerd zijn en niets met corona te maken hebben.

**Berndt verlaat meeting**

(10)(2e) : *Het plan van Aanpak voor de WOB-verzoeken* gaat de scope hebben van het doorzoeken van mailboxen van de crisisorganisatie Corona.
(10)(2e) Project Corona Archivering gaat iets breder. Veel directies geven aan weldegelijk iets te doen met Corona. En vragen ons dit te onderzoeken. Dus ook (delen van) niet-crisisorganisaties worden onderzocht.

(10)(2e) : Wij moeten waarborgen dat het gaat om bij Corona betrokken organisaties, dat directies zelf toestemming geven en we altijd beginnen met netwerkschijven (bevat merendeel informatie), dat alleen mailboxen van specifieke functionarissen worden doorzocht en dat we in overleg met directie/afdeling bepalen welke mappen en welke medewerkers moeten worden doorzocht.

(10)(2e) : De directie moet worden geïnformeerd en hun medewerkers ook. Men moet 'nee' kunnen zeggen. Denk ook na over dataminimalisatie: heb ik alles echt nodig? We willen niet slecht in de pers komen.

(10)(2e) : (Vraag aan (10)(2e) ) We hebben WOB-verzoeken liggen en de wettelijke plicht om deze binnen 8 weken te beantwoorden. Is dit nog mee te nemen in de onderbouwing?
(10)(2e) : Jazeker. Je zou voor de onderbouwing kunnen kijken naar bijvoorbeeld in algemeen belang. Artikel 6 e algemeen belang van AVG. Op bijzondere persoonsgegevens zit een verbod. Voor het doorbreken van dit verbod moet wel een zeer goede grondslag voor zijn.
**Actie:** (10)(2e) vraagt na bij jurist van WJZ hoe zij zijn omgegaan met e-mailarchivering Rijksbreed. Daar ook vraagstuk naar voren van doorbereken medisch beroepsgeheim.

**Afronding**

(10)(2e)

- gaat het memo aanpassen;
- gaat keuze voorleggen aan opdrachtgever n.a.v. dit overleg.

(10)(2e): Advies om zeker de procedure / Quickscan te doorlopen.

(10)(2e): *Het memo* moet ook langs adviseur van de SG. De inhoud mag geen vragen opwerpen (bij een leek). Als iets vragen oproept, verduidelijk dit dan. Bijvoorbeeld: Welke beschikbare software? Welke koppelingen? Draaien er al koppelingen en waarom? Ook moeten alle et cetera's weg uit de tekst.
(10)(2e): De Quickscan ontvangen we heel graag. Dan gaan we kijken hoe ver we daar mee komen. Als er input nodig is dan komen we bij jullie terug.
(10)(2e): Quickscan kan (10)(2e) bij helpen, maar I-team is hierin meer bedreven.
(10)(2e): (10)(2e), ga (10)(2e) helpen.

(10)(2e)

- We maken een gespreksverslag;
- We gaan aan de slag met een 2e versie (ruw) van het memo;
- We vullen de QuickScan in (hiaten later invullen) en aan onze opdrachtgever de status doorgeven en praten over tempo;
- Volgende week donderdag risicoanalyse op de mailboxen. (10)(2e) gaat bellen of wij hierin betrokken kunnen worden.

12:50 afsluiting