Auditdienst Rijk
Ministerie van Financiën

SG-Cluster
Auditdienst Rijk

TER BESPREKING
Aan
de voorzitter en de leden van het overleg van secretarissen-generaal

Datum
24 oktober 2023

Notanummer
2023-0000224561

Bijlage
Goede praktijkvoorbeelden interim-rapportages 2023

nota

Tussentijds rijksbreed beeld ADR 2023

1. Inleiding

In deze nota schetsen wij ons tussentijdse rijksbrede beeld over 2023. Dit is gebaseerd op de kennis en inzichten die wij hebben opgedaan bij onze onderzoeken voor de Rijksdienst in de eerste helft van dit jaar. In de bijlage hebben wij een aantal goede praktijkvoorbeelden uit onze interim-rapportages 2023 opgenomen op het terrein van financieel beheer, IT-beheer en informatiebeveiliging.

Belangrijke aandachtspunten:
- investeer meer in de beheersing, verantwoording en evaluatie van kunstmatige intelligentie;
- doorbreek de situatie waarin onvoldoende tempo gemaakt wordt met de aanlevering van kwalitatief voldoende informatie voor de aanspraak op HVP-gelden van de Europese Unie;
- breng de privacyrisico's binnen het departementale cloudbeleid beter in kaart;
- inventariseer wat er nodig is om te voldoen aan de tweede Europese netwerk- en informatiebeveiligingsrichtlijn en reserveer hiervoor tijdig capaciteit;
- bundel en vereenvoudig de subsidie-uitvoering binnen het Rijk; maak operationele afspraken om het risico op fouten en onbedoelde effecten te verkleinen;
- trek samen op voor de rijksbrede werving van (tijdelijk) personeel en investeer in maatregelen die de arbeidsproductiviteit bij het Rijk verhogen;

2. Verantwoorde inzet van kunstmatige intelligentie

In ons rijksbrede tussentijdse beeld van 2022 constateerden wij dat besluitvorming met behulp van algoritmen en (generatieve) kunstmatige intelligentie (AI)[1] vraagt om zorgvuldige beheersings- en verantwoordingsprocessen. Hier schort het nogal eens aan. Zelfs als de doelen, overwegingen en keuzes rondom de inzet van het algoritme aan de voorkant goed zijn onderbouwd, blijken deze vaak beperkt te zijn vastgelegd. Daarnaast zijn de criteria (o.a. op het gebied van acceptatie en prestatie) waaraan het algoritme moet voldoen meestal niet vooraf bepaald. Dit maakt het voor organisaties lastig om te monitoren en evalueren hoe het algoritme functioneert, welke risico's na verloop van tijd ontstaan, hoe hiermee om te gaan en hoe hierover verantwoording kan worden afgelegd. Maar het belang van adequate risicobeheersing neemt alleen maar toe, zo stelt ook de Autoriteit

[1] Kunstmatige of artificiële intelligentie is een verzameling algoritmen in een systeem dat gegevens en regels gebruikt om beoordelingen of voorspellingen te doen. Generatieve AI is een technologie die op grond van een menselijke vraag of opdracht automatisch een tekst, afbeelding of video creëert.

Persoonsgegevens in haar rapportage van juli 2023.[2] Het AI-veld ontwikkelt zich immers snel; algoritmen worden steeds krachtiger en generatieve AI zoals ChatGPT zijn steeds breder toegankelijk.

Over de beheersing, verantwoording en evaluatie van AI adviseren wij departementen en uitvoeringorganisaties:
- zorg dat afwegingen tussen maatschappelijke waarden zorgvuldig gemaakt worden en er voldoende aandacht is voor de data-ethische aspecten van het algoritme;
- zorg dat algoritmen worden gepubliceerd in het – in de toekomst wettelijk verplichte - algoritmeregister voor de overheid, zodat ze gecontroleerd kunnen worden;
- richt een werkend en gedocumenteerd proces in voor periodieke evaluatie van de kwaliteit van het algoritme. Deel de resultaten hiervan met belanghebbenden;
- analyseer of (interne en externe) klachten en incidenten het gevolg kunnen zijn van het gebruik van het algoritme en zorg dat het algoritme snel aangepast kan worden wanneer het niet wenselijk presteert;
- creëer een cultuur waarin transparantie en het leren van evalueren voorop staan. Hierdoor kunnen blinde vlekken en mogelijke fouten of problemen in systemen sneller aan het licht komen en gecorrigeerd worden.

3. Herstel- en Veerkrachtplan

Vorig jaar heeft de Raad van de Europese Unie (EU) het Nederlandse Herstel- en Veerkrachtplan (HVP) voor duurzaam economisch herstel goedgekeurd. In onze hoofdlijnennotitie van oktober 2022 constateerden wij dat de departementen nog veel werk moesten verzetten om de eerste betaalaanvraag bij de Europese Commissie met succes te kunnen indienen.

Onze recente controles van de informatie die de departementen medio juni van dit jaar hebben aangeleverd, wijzen uit dat Nederland onvoldoende voortgang heeft geboekt om volgens plan in december 2023 in aanmerking te kunnen komen voor de eerste betaling (1,3 miljard euro van het totaalbedrag van 4,7 miljard euro). Hoewel de departementen behoorlijk wat werk verrichten, leidt dit nog niet tot het niveau van oplevering van informatie dat vanuit de Europese Commissie wordt gevraagd. Wij constateren het volgende:
- de opgeleverde HVP-procesbeschrijvingen van onder meer de risicoanalyses en de beheer- en controlemaatregelen zijn onvoldoende toegespitst op de afzonderlijke HVP-maatregelen;
- de vereiste informatie over eindbegunstigden en contractanten in het voorgeschreven centrale dataregister is nog onvoldoende beschikbaar. Hierdoor zijn er nog geen werkzaamheden uitgevoerd op het door de EU vereiste detailniveau om fraude, corruptie, dubbele financiering en belangenverstrengeling te voorkomen;
- er is alleen eenvoudige informatie omtrent het behalen van mijlpalen aangeleverd, zoals afgesloten contracten. Kwantitatieve onderbouwingen van de mijlpalen ontbreken of zijn onvolledig. Ook is er nog geen aansluiting gemaakt op de administratie;
- de controles van de eerste en tweede lijn zijn onvoldoende zichtbaar uitgevoerd.

Inmiddels is besloten het eerste betaalverzoek in mei 2024 in te dienen. Hierdoor ontstaat ruimte voor een nieuwe aanlevering, validatie en controle voor het eerste betaalverzoek. Zonder stevige aanvullende maatregelen is het echter

[2] Autoriteit Persoonsgegevens, publicatie "Toezicht op AI & Algoritmes". De ADR heeft een praktisch, risicogericht onderzoekskader ontwikkeld voor zowel regelgebaseerde als zelflerende algoritmen om de algehele beheersing ervan bij overheidsorganisaties in kaart te brengen.

onwaarschijnlijk dat de vereiste kwaliteit van de verantwoording en de bijbehorende onderbouwingen dan wél geleverd gaat worden. Eerdere pogingen om hieraan prioriteit te geven hebben immers weinig effect gehad.

Via een getrapt systeem van deelverklaringen per betrokken beleidsdirectie dient uiteindelijk de Secretaris-Generaal (SG) de departementale beheersverklaring te ondertekenen. Hiermee onderkent de SG de verantwoordelijkheid voor het beschermen van de financiële belangen van de Unie en staat garant voor de betrouwbaarheid van de aangeleverde gegevens aan de programmadirectie HVP.

Indien de kwaliteit van de verantwoording onder de maat blijft, zullen de individuele departementen hiervan zelf de financiële tegenvallers moeten opvangen. Wij adviseren de departementen de situatie waarin onvoldoende tempo gemaakt wordt te doorbreken en te voorkomen dat de volgende aanlevering van informatie wederom ver beneden de maat scoort. Te denken valt aan het instellen van een regiefunctie – met een passende mix van centrale en departementale elementen - die niet alleen coördineert, maar ook beschikt over het mandaat, de doorzettingsmacht én de actieve medewerking van en binnen de betrokken departementen. Op deze wijze kan in een aantal maanden het best mogelijke resultaat geboekt worden.

4. Privacy-aspecten van clouddiensten

Eind 2022 is het rijksbreed cloudbeleid vastgesteld. Dit vormt een belangrijke stap in de noodzakelijke uniformering en professionalisering van het omgaan met commerciële (publieke) clouddiensten en -dienstverleners. Een aantal privacyrisico's in dit beleid en in de uitvoering blijven echter nog altijd onderbelicht. Het betreft onder meer risico's voorafgaand aan de vraag of een (publieke) clouddienst rechtmatig kan worden ingezet, extra risico's die ontstaan bij de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (EER) en risico's van het daadwerkelijke gebruik van de cloud door de departementen.

Begin 2023 heeft de ADR het *Rijksbreed AVG onderzoek 2022* aangeboden aan de CIO-Rijk. Hierin zijn ook de privacy-criteria in de departementale cloudstrategieën onderzocht. Naar aanleiding hiervan adviseren wij de Chief Information Officers (CIO's) en de CIO-Rijk:

- de privacyrisico's binnen de uitvoering scherper in kaart te brengen, zeker bij grote niet-Europese leveranciers.
- extra aandacht te schenken aan de classificatie van gegevens, het eigenaarschap in het kader van de exit-strategie en de locatie van data, vooral wanneer deze buiten de EER worden opgeslagen.

De ADR gaat op verzoek van de CIO Rijk het rijksbreed cloudbeleid evalueren.

5. Impact NiB2-richtlijn op Rijksoverheid

De tweede netwerk- en informatiebeveiligingsrichtlijn (NiB2) van de Europese Unie beoogt het niveau van cyberbeveiliging en weerbaarheid van leveranciers van essentiële diensten in EU-lidstaten te verhogen en bij te dragen aan meer Europese harmonisatie. Ook overheidsdiensten vallen onder deze richtlijn. Europese lidstaten hebben tot eind 2024 de tijd om deze om te zetten in nationale wetgeving. Er komen strengere eisen ten aanzien van onder meer:

- de zorgplicht: organisaties zijn verplicht een risicobeoordeling uit te voeren en vervolgens passende maatregelen te nemen om hun diensten te waarborgen en gebruikte informatie te beschermen tegen cyberrisico's;
- de meldplicht: organisaties moeten incidenten die de verlening van essentiële diensten (kunnen) verstoren binnen 24 uur melden bij de toezichthouder. Een cyberincident dient ook gemeld te worden aan het *Computer Security Incident Response Team*;

- toezicht: organisaties komen onder toezicht te staan. De toezichthouder onderzoekt de naleving van de verplichtingen uit de richtlijn, waaronder de zorg- en meldplicht.

Een groot deel van de eisen omtrent de zorgplicht voor de overheid zullen naar verwachting worden opgenomen in de Baseline Informatiebeveiliging Overheid (BIO) 2.0. Deze zal uiterlijk in oktober 2023 van kracht worden. Het niet naleven van de NiB2-richtlijn kan zowel financiële als juridische gevolgen hebben. Organisaties kunnen boetes krijgen en bestuurders kunnen juridische stappen tegemoet zien en hoofdelijk aansprakelijk worden gesteld. Ook kan de reputatie en geloofwaardigheid van de Rijksoverheid worden geschaad. Uit onze eigen informatiebeveiligingsonderzoeken[3] en onderzoek in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties[4] blijkt dat juist het risicomanagement en het *aantoonbaar* voldoen aan de belangrijkste informatiebeveiligingsmaatregelen de afgelopen jaren tekortschoten.

Wij adviseren het management van de rijksorganisaties, eventueel ondersteund door de Chief Information Security Officers:
- na te gaan welke stappen nodig zijn om te voldoen aan de NiB2-richtlijn en hiervoor tijdig voldoende capaciteit vrij te maken;
- het strategisch risicomanagement te versterken door in het drielijnenmodel[5] nadrukkelijk ook de informatiebeveiliging op te nemen.

6. Uitvoering subsidies: versnipperd, complex, hoge beheerlast

De subsidie-uitvoering binnen het Rijk is versnipperd. Er zijn ongeveer 750 verschillende subsidieregelingen naast individuele instellings- en projectsubsidies, en dat aantal groeit nog steeds. Iedere individuele subsidieregeling heeft eigen rechtmatigheids- en verantwoordingseisen. Rijksbreed zijn hier zo'n 30 uitvoeringsprocessen en (IT-)systemen van zo'n tien verschillende (uitvoerings)organisaties en diverse beleidsdirecties per departement mee gemoeid. Het kost de departementen veel tijd en geld om de diverse processen en systemen in de lucht te houden. Ook het correct uitvoeren van al deze regelingen is complex, arbeidsintensief en vraagt specifieke expertise. In een steeds krappere arbeidsmarkt wordt het moeilijker voldoende en goed geschoolde medewerkers aan te trekken en te behouden. Bovendien brengt het complexe landschap van regelingen voor de aanvragers van subsidies extra lasten en risico's op fouten met zich mee, zo stelt ook de *Staat van de uitvoering 2022*.

Wij adviseren de departemensleiding:
- te overwegen de subsidie-uitvoering binnen het Rijk centraler aan te pakken en te vereenvoudigen, bijvoorbeeld door meer regelingen onder te brengen bij grote uitvoeringsorganisaties zoals DUO, UWV en RVO. Dit leidt tot schaalvoordelen waardoor de beheerlast kan dalen, kennis gebundeld kan worden en de uitvoering en controle efficiënter en stabieler worden;
- operationele afspraken met beleidsdirecties en uitvoeringsorganisaties te maken over het verzamelen van, en handelen naar signalen van dubbele aanvragen of onderbenutting, foutieve aanvragen, stapeling, misbruik of oneigenlijk gebruik van regelingen.

---

[3] Auditdienst Rijk, Rijksbreed onderzoek beheersing informatiebeveiliging 2020, 2019 en 2018.
[4] Berenschot, Onderzoek Sturen op informatieveiligheid.
[5] De eerstelijnsrol betreft het lijnmanagement van de (beleids)directies, die verantwoordelijk is voor de eigen processen. De tweedelijnsrol heeft betrekking op het adviseren, ondersteunen, coördineren en bewaken dat het lijnmanagement deze verantwoordelijkheden ook daadwerkelijk neemt. De directie FEZ van de departementen vervult deze tweedelijnsrol op het terrein van het begrotings- en financieel beheer; voor de andere terreinen van de bedrijfsvoering is de tweedelijnsrol elders in de departementale organisatie belegd.

7. Arbeidsmarktkrapte en tegengaan van schijnzelfstandigheid

Nederland kampt sinds enkele jaren met een arbeidsmarktkrapte van historische omvang. Omdat de onderliggende vergrijzing nog decennia zal doorwerken, vormt dit een risico voor de continuïteit en kwaliteit van de (semi)publieke dienstverlening en de aanpak van grote maatschappelijke vraagstukken. Goed arbeidsmarktbeleid kan een bijdrage leveren aan het verminderen van de krapte, zo blijkt uit diverse analyses.

Het arbeidsmarktbeleid probeert al jaren de onwenselijke verschillen in behandeling tussen uiteenlopende arbeidsrelaties (vast dienstverband, zelfstandig, uiteenlopende vormen van tijdelijke contracten) te verkleinen en schijnzelfstandigheid[6] tegen te gaan. Het fiscaal onderscheiden van, en handhaven bij schijnzelfstandigheid blijkt al sinds de invoering van de Wet Deregulering beoordeling arbeidsrelaties (DBA) in 2016 op principiële en praktische problemen te stuiten. Daarom is al bij de invoering van de wet besloten opdrachtgevers alleen naheffingen en boetes op te leggen als evident sprake is van kwaadwillendheid (het zogenoemde 'handhavingsmoratorium'). In de reactie op onderzoek van de Algemene Rekenkamer en de ADR kondigde het kabinet medio 2022 aan het handhavingsmoratorium op de Wet DBA per 1 januari 2025 op te heffen.[7] Ook gaan de ministeries zelf sturen op beëindiging van de inhuur van schijnzelfstandigen, verambtelijking van de inhuur en herinrichting van werkzaamheden.

Wij adviseren:
- gezamenlijk op te trekken in de rijksbrede werving van (tijdelijk) personeel, om te voorkomen dat rijksoverheidsorganisaties elkaar onderling beconcurreren en om te ontmoedigen dat payroll partijen zzp'ers blijven aanbieden als tijdelijke krachten;
- meer te investeren in productiviteitsverhogende maatregelen, zoals het werk slimmer organiseren, verder digitaliseren, meer regelruimte creëren en de stapeling van beleid aan te pakken.

[6] Schijnzelfstandigen zijn gedefinieerd als werkenden die zich presenteren als zelfstandigen zonder personeel (zzp'er) maar op basis van de wet- en regelgeving kwalificeren als werknemer en dus eigenlijk een dienstverband zouden moeten hebben.

[7] Zie: Algemene Rekenkamer, Focus op handhaving Belastingdienst bij schijnzelfstandigheid , ADR, Onderzoeksrapport evaluatie uitvoering toezichtplan arbeidsrelaties en de reactie op beide rapporten in de Kamerbrief.

BIJLAGE: GOEDE PRAKTIJKVOORBEELDEN INTERIM-RAPPORTAGES 2023

Financieel beheer

BZ: voortgang programma 'versterking BZ in control'

Dit jaar heeft BZ verdere voortgang gemaakt met het versterken van de interne beheersing als onderdeel van het programma 'Versterking BZ in control'. De directie FEZ heeft eerstelijnsdirecties en ODA[8]-posten onder meer gecommitteerd aan het (tijdig) opleveren van een risicoanalyse en interne beheersmaatregelen, een self-assessment (pilot voor de posten) voor het verkrijgen van inzicht hierin en het periodiek uitvoeren van verbijzonderde interne controlewerkzaamheden (VIC's). Deze VIC's hebben als doel aantoonbaar vast te kunnen stellen dat de directie/post in control is of dat bijsturing nodig is. FEZ monitort de tijdige ontvangst van bovengenoemde producten en geeft hiervan (op onderdelen) een appreciatie.

BZK: versterking van het Three Lines model

De directie FEZ van BZK investeert in risicoanalyses voor de processen, interne beheersingsmaatregelen en toetsing daarvan in de eerste lijn. Met monitoring en handhaving vanuit de tweede lijn op de interne beheersing door de eerste lijn zal de Plan-do-check-act (PDCA)-cyclus worden gesloten en wordt het Three Lines model versterkt. Dit zal BZK in staat stellen om zelf tijdig bij te sturen in het financieel beheer om bevindingen in de interne beheersing en fouten in de rechtmatigheid te voorkomen. Ook bij de uitvoeringsorganisaties zijn er ontwikkelingen op dit vlak.

J&V: verdieping van de concernbrede fraudeanalyse

De directie FEZ van J&V heeft medio 2022 een eerste concernbrede frauderisicoanalyse opgeleverd. Dit jaar is hierop een belangrijke verdiepingsslag aangebracht door met twaalf J&V-organisaties, onder andere de agentschappen en de shared service centra, het gesprek aan te gaan over fraude- en corruptie-risico's. FEZ heeft deze organisaties gestimuleerd om nog ontbrekende inschattingen te maken van de kans en impact van de benoemde frauderisico's en om de ingerichte beheersmaatregelen vast te leggen.

VWS: fundament voor robuust financieel beheer gelegd

Het verbetertraject 'Structurele en culturele borging' bij VWS levert zichtbare resultaten op. Wij zien in 2023 een duidelijke aanscherping van de invulling van de rollen van het Three Lines model. De directie FEZ pakt haar kaderstellende en monitorende rol beter op en spreekt de beleidsdirecties meer aan op hun verantwoordelijkheid voor een goed financieel beheer en een goede financiële administratie. Zo is FEZ gestart met de uitvoering van interne controles en worden opvallende zaken wekelijks besproken met de financieel adviseurs per kolom. Ook is VWS gestart met de pilot data-analyse (als onderdeel van het programma Toekomst Financiële Administratie van het ministerie van Financiën) om zo op efficiënte en snelle manier (mogelijke) fouten in de administratie te kunnen opsporen. De betrokkenheid van de ambtelijke leiding via de regiegroep heeft een positief effect op de aandacht van de VWS-organisatie om de bedrijfsvoering naar het gewenste niveau te brengen.

[8] Official Development Aid.

Financiën: doorontwikkeling van toezicht op het financieel beheer

Het in 2022 gestarte programma Toezicht en Advies Financieel Beheer is afgerond en overgedragen aan de lijn. Dit jaar heeft de directie FEZ de eerste ervaringen opgedaan met tussentijds afsluiten, gericht op risicovolle onderdelen in de administraties, het corrigeren van onjuiste boekingen en het tijdig afstemmen van verslaggevingsvraagstukken. Een tweede tussentijdse afsluiting is momenteel onderhanden. Coördinatie van het jaarverslagproces vindt plaats vanuit een begeleidingscommissie. Doel is om het jaarverslagtraject beter te stroomlijnen, onder meer door delen van de controle te dynamiseren. Door controlewerkzaamheden eerder in het jaar uit te voeren, wordt de druk op de jaarafsluiting verminderd.

IT-beheer en informatiebeveiliging

BZK: verbeteringen bij SSC-ICT en stappen gezet voor rijksbrede IT-beheer

In 2023 heeft SSC-ICT het verbeteren van de informatiebeveiliging aantoonbaar doorgezet. Dit blijkt uit de hogere kwaliteit van het Internal Control Framework, het bijbehorend beheersingsproces en het toevoegen van meer systemen aan dit framework. SSC-ICT heeft de interne auditfunctie verder versterkt en geïnvesteerd in het geheel van maatregelen en processen voor de betrouwbaarheid van de informatiebeveiliging. Dit is terug te zien in het risicomanagement, de aandacht voor en verbetering van de beveiliging van componenten, de interne auditplanning en de nadere uitwerkingen van de doelstellingen vanuit het beleidsdocument voor Security Informatie & Event Monitoring.

Het directoraat-generaal Digitalisering en Overheidsorganisatie van BZK heeft verdere stappen gezet ten aanzien van de rijksbrede regiefunctie van IT-beheer. Afgelopen zomer is een plan van aanpak voor rijksbreed IT-beheer goedgekeurd om te komen tot een PDCA-cyclus waarin departementen, agentschappen en ICT-dienstverleners de CIO Rijk periodiek gaan informeren over de wijze waarop zij hun IT beheren.

Defensie: effecten programma Grensverleggende IT zichtbaarder

De contouren en gevolgen van het Programma Grensverleggende IT (GrIT) worden zichtbaar binnen het huidige IT-domein van Defensie. Er vinden continue veranderingen plaats die leiden tot implementatie van nieuwe IT-componenten en/of IT-processen binnen het bestaande IT-domein. Tot de definitieve migratie naar de nieuwe datacenters van Defensie vereisen de ontstane parallelle IT-infrastructuren binnen het huidige IT-domein een goede communicatie en afstemming.