Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Strategische I-agenda Rijksdienst 2019-2021, *editie 2020*

Dit is een uitgave van CIO Rijk in samenwerking met het CIO-beraad

Inhoudsopgave

1 Inleiding

Nederland wil digitaal koploper van Europa worden[1] en wil een pionier zijn voor verantwoorde digitale innovatie[2]. Overheidsbreed is innovatie ook een belangrijk thema, naast onder meer data. De overheid wil data (beter) inzetten om maatschappelijke opgaven aan te pakken[3,4]. Daarbij is goede informatiebeveiliging essentieel om veilig te kunnen werken[5,6]. Zoals ook de Europese Commissie recent heeft benoemd, biedt digitalisering dus zowel kansen als bedreigingen[7]. De Rijksdienst heeft daarom de uitdaging om samen rijksbreed de informatievoorziening (IV), data, ICT en informatiebeveiliging te versterken, om bij te dragen aan maatschappelijke vraagstukken en de ambities, zoals verwoord in de Agenda Digitale Overheid (NL DIGIbeter). Ook wordt aansluiting gezocht met de werkagenda voor de uitvoering van de Ministeriële Commissie Uitvoering (MCU), die door het kabinet is ingesteld. De minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft in 2019 en haar visie op informatiebeveiliging, ICT en de organisatie binnen de Rijksdienst daarvan beschreven in twee Kamerbrieven[8,9], die in deze Strategische I-agenda Rijksdienst verder worden uitgewerkt[10].

De ambitie bij de Rijksdienst is om met informatievoorziening, data, ICT en informatiebeveiliging voorop te lopen en kansen te benutten, waarbij iedereen meedoet en samenwerking binnen de Rijksdienst van groot belang is, met vertrouwen in de digitale toekomst.

De CIO's (Chief Information Officers) binnen de Rijksdienst hebben in hun organisatie uiteenlopende taken en verantwoordelijkheden en eigen maatschappelijke opgaven. Zij worden daarbij ondersteund door onder andere een CISO (Chief Information Security Officer) voor informatiebeveiliging. Organisaties die zelf ICT-diensten leveren, hebben daarnaast ook een CTO (Chief Technology Officer). Deze Strategische I-agenda Rijksdienst beschrijft de Rijksbrede activiteiten van de gezamenlijke CIO's, gericht op stimuleren wat al goed loopt, versterken waar dat nodig is en leren van elkaar en anderen. Ze kunnen kansen signaleren en mogelijke ontwikkelingen agenderen. Het ministerie van BZK is aanjager, verbinder en platform voor kennisdeling. De CIO's, CTO's en CISO's gaan uit van een open cultuur waarin fouten besproken kunnen worden en waarin successen gedeeld kunnen worden, ook al zijn ze niet altijd (breed) zichtbaar.

---

[1] Regeerakkoord 'Vertrouwen in de toekomst', Bijlage bij *Kamerstukken II* 2017/18, 34700, nr. 34
[2] Nederlandse Digitaliseringsstrategie 2.0, bijlage bij *Kamerstukken II* 2018/19, 26643, nr. 623
[3] Agenda Digitale Overheid, NL DIGIbeter, editie 2019, *Kamerstukken II* 2018/19, 26643, nr. 621
[4] NL DIGItaal, de Data Agenda Overheid, *Kamerstukken II* 2018/19, 26643, nr. 597
[5] Cybersecuritybeeld Nederland 2019, *Kamerstukken II* 2018/19, 26643, nr. 614
[6] 'Voorbereiden op Digitale Ontwrichting' van de Wetenschappelijke Raad voor het Regeringsbeleid, https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting
[7] "A Union that strives for more", Ursula von der Leyen, Political guidelines for the next European Commission 2019-2024
[8] *Kamerstukken II* 2018/19, 26643, nr. 573
[9] *Kamerstukken II* 2019/20, 26643, nr. 656
[10] Meer informatie over de documenten waarnaar wordt verwezen is te vinden in de bijlage Context Strategische I-agenda Rijksdienst

Strategische I-agenda en ontwikkeling opvolger
In 2011 is de Rijksbrede I-Strategie[11] verschenen, die voortkwam uit het programma Compacte Rijksdienst. Deze I-Strategie had een looptijd van vier jaar. Vijf jaar later is ervoor gekozen om een meerjarige Strategische I-agenda Rijksdienst[12] op te stellen die jaarlijks wordt geactualiseerd. Begin 2019 is de Strategische I-agenda Rijksdienst voor de planperiode 2019-2021[13] verschenen en later dat jaar is de Kamer geïnformeerd over de voortgang[14]. De voorliggende I-agenda, editie 2020, houdt dezelfde planperiode aan.

De Strategische I-agenda richt zich op de informatievoorziening bij de Rijksdienst, waarbij ICT – de meer technische kant - een onderdeel is van informatievoorziening. Daarnaast is informatiebeveiliging een belangrijk aspect. De filosofie van de I-agenda is om met kleine stappen een grote sprong te maken en per jaar te bezien of we nog op de goede weg zitten. Dat geeft ruimte om innovatieve ontwikkelingen tijdens de looptijd samen uit te denken.

De I-agenda bevat zowel strategische- als operationele aspecten. Komende jaren wordt toegewerkt naar een opvolger van dit document op een hoger abstractieniveau dan de huidige I-agenda. Die opvolger zal een aantal thema's met concrete doelstellingen bevatten. Daarnaast zal een overkoepelende routekaart worden opgesteld met een meer operationele focus, met daaronder routekaarten per thema. Deze routekaarten geven aan welke stappen de Rijksdienst gaat zetten om de doelen te bereiken.

Samenvatting en leeswijzer
Deze I-agenda start in het tweede hoofdstuk met ***informatiebeveiliging en privacy***. Elk ministerie heeft een Chief Information Security Officer (CISO), voor deze rol wordt een profiel opgesteld. Dit profiel wordt beschreven in samenhang met de creatie van de CISO Rijk binnen het ministerie van BZK. De Privacy Adviseur Rijksbrede Kaders en Voorzieningen (PAR) zorgt voor zorgvuldige omgang met persoonsgegevens binnen Rijksbrede trajecten. Het ministerie van BZK faciliteert het vergroten van de kennis over privacy binnen de Rijksdienst.

Het derde hoofdstuk gaat over de ***informatiehuishouding en data*** van de Rijksdienst. Voor informatiehuishouding heeft het Kabinet een forse ambitie neergezet. Hierbij gaat het onder andere om het beter veiligstellen van informatie, meer actieve openbaarmaking, kortere overbrengingstermijnen naar het Nationaal Archief en meer kennisdeling over informatiehuishouding. Rondom data worden initiatieven bij elkaar gebracht, verkenningen uitgevoerd en kennis gedeeld.

In het vierde hoofdstuk komt ***ICT*** aan de orde. Er is een aantal gemeenschappelijke ICT-voorzieningen voor de Rijksdienst, waaronder een aantal gericht op informatiebeveiliging. In dit hoofdstuk komt ook de afweging aan bod tussen het zelf uitvoeren of laten uitvoeren van werkzaamheden op ICT-gebied. Hierbij wordt ook gebruik van de *cloud* verkend. De Rijksdienst investeert doorlopend in de relatie met commerciële partijen en werkt aan verduurzaming van ICT-inkoop. Tenslotte is er in dit hoofdstuk aandacht voor *levenscyclusmanagement*.

Het vijfde hoofdstuk draait om het vergroten van ***kennis en kunde*** op het gebied van informatievoorziening, ICT en informatiebeveiliging binnen de Rijksdienst. Denk hierbij aan de ontwikkeling en verbinding van kennis en kunde binnen de I-community van de Rijksdienst, het

[11] *Kamerstukken II* 2011/12, 26643, nr. 216
[12] *Kamerstukken II* 2016/17, 31490, nr. 221
[13] *Kamerstukken II* 2018/19, 26643, nr. 591
[14] *Kamerstukken II* 2019/20, 26643, nr. 646

versterken van digitaal bewustzijn en digitale vaardigheden bij beleidsmakers en het versterken van het Rijk als ICT-werkgever.

Het zesde en laatste hoofdstuk richt zich op het ***versterken van het CIO-stelsel*.** Dit hoofdstuk bevat een beschrijving van
instrumenten om de ambities uit de I-agenda waar te maken. Deze instrumenten liggen onder andere op het gebied van organisatie, planvorming en transparantie.

2 Informatiebeveiliging en privacy

2.1 Informatiebeveiliging

De samenleving en de overheid worden steeds digitaler. Dit brengt nieuwe bedreigingen met zich mee die om nieuwe oplossingen vragen. De Rijksdienst moet daarom voortdurend en intensief aandacht geven aan informatiebeveiliging.

Er vindt monitoring plaats op de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)[15] en waar mogelijk wordt de feitelijke veiligheid van de informatievoorziening van de Rijksdienst bevorderd. Uitgangspunten daarbij zijn continuïteit van vitale systemen en de toepassing van maatregelen die passen bij het noodzakelijke beveiligingsniveau van informatie. Met name waar het gaat om het hoogste basisbeveiligingsniveau (basisbeveiligingsniveau 3, BBN3), dat weerbaarheid moet bieden tegen dreigingen van statelijke actoren, is geconstateerd dat maatwerk is vereist. Ministeries doen dit bijvoorbeeld door het implementeren van een geschikte set van beveiligingsmaatregelen uit de geldende EU- en NATO-kaders. Aangezien onvoldoende toegevoegde waarde wordt verwacht van een algemene Rijksbrede standaard voor BBN3 wordt afgezien van uitbreiding van de BIO op dit punt. Indien daar in een later stadium toch behoefte aan blijkt te bestaan bij de Rijksdienst of bij andere bestuurslagen, zal dit in het reguliere onderhoudsproces van de BIO worden meegenomen.

Er zal Rijksbreed meer aandacht worden besteed aan goede toepassing van rubricering van informatie. Hiermee wordt bepaald hoe zwaar een gegeven beveiligd moet worden, waardoor ambtenaren intuïtiever zorgvuldig met gevoelige informatie kunnen omgaan.

In 2020 wordt de bijdrage aan het Nationaal Cyber Security Centrum (NCSC) om meer partijen op het Nationaal Detectie Netwerk (NDN) aangesloten te krijgen gecontinueerd. Inmiddels is sprake van een 71% dekkingsgraad, waarbij gestreefd wordt om binnen de planperiode van de I-agenda een volledige dekking te realiseren.

In overleg met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het NCSC wordt verder verkend hoe het proces van doorlopende kwetsbaarhedenscan door rijksoverheidsorganisaties verder kan worden ingericht en versterkt. Hierbij zal in 2020 worden ingezet op een Rijksbreed kader.
Uit de reactie van het kabinet op het WRR-rapport[16] volgt nog een aantal concrete acties voor CIO Rijk en het CIO-beraad, die samen met de NCTV worden uitgewerkt in het Nationaal Crisisplan (NCP). Zo zullen de komende periode, naast de al bestaande richtlijnen en kaders, bindende afspraken gemaakt worden over het leveren van inzicht in de toegepaste netwerk- en informatiesystemen.

Elk ministerie heeft een Chief Information Security Officer (CISO), maar de CISO-taken zijn nu niet Rijksbreed geformaliseerd en wisselen per ministerie. De CISO heeft sterke relaties met de CIO en de Beveiligingsambtenaar die in elk ministerie aanwezig zijn. In 2020 wordt de minimaal in te vullen set taken van de departementale CISO Rijksbreed geformaliseerd. Dit traject heeft een relatie met de ontwikkeling van een Besluit CIO-stelsel Rijksdienst (zie Versterken van het CIO-stelsel) en de creatie van de Chief Information Security Officer Rijk (CISO Rijk) binnen het ministerie van BZK[17]. De CISO Rijk zal zorgen voor de integrale borging

[15] Tot stand gekomen op basis van de BIR 2017, BIR staat voor Baseline Informatiebeveiliging Rijksdienst
[16] *Kamerstukken II* 2019/20, 26643, nr. 673
[17] *Kamerstukken II* 2018/19, 26643, nr. 620

van informatiebeveiliging binnen het Rijksbrede ICT-beleid. In 2020 is de werving voor de CISO Rijk gestart.

2.2 Privacy

De digitalisering van de samenleving en de overheid heeft tot nieuwe mogelijkheden voor het verwerken en koppelen van gegevens geleid, en daarmee tot nieuwe vragen op het gebied van privacy. Daarom is de rol van Privacy Adviseur Rijksbrede Kaders en Voorzieningen (PAR) ingesteld. De PAR adviseert bij besluitvorming over verwerking van persoonsgegevens binnen interdepartementale bedrijfsvoeringprocessen. De PAR-procedure is in 2018 gestart en wordt in 2020 geëvalueerd..

Het ministerie van BZK faciliteert het vergroten van kennis over privacy binnen de Rijksdienst, door het delen van kennis en ervaringen uit de dagelijkse praktijk en bijvoorbeeld in voorbereiding op de komende E-Privacy Verordening. Dit versterkt de samenwerking tussen en met de Functionaris Gegevensbescherming, privacy officers en privacy juristen. In 2020 zal de primaire focus liggen op het, in afstemming met de departementen, opstellen van privacy-adviezen voor Rijksbrede trajecten. De Rijksbrede privacy ondersteuning van departementen zal worden gecontinueerd, onder meer door het organiseren van kennissessies en het door-ontwikkelen van het rijksmodel voor Privacy impact Assessments (PIA) en de quick scan PIA. Daarnaast wordt waar mogelijk gewerkt aan de integratie van informatiebeveiliging en privacy voor risicomanagement en Rijksbrede kaders.

3 Informatiehuishouding en data

3.1 Informatiehuishouding

De Rijksdienst heeft een goede informatiehuishouding nodig om haar taken uit te voeren. Daarnaast kunnen burgers, bedrijven en het parlement hierdoor de Rijksdienst controleren. Het kabinet wil de informatiehuishouding met het richtinggevende 'Meerjarenplan verbetering informatiehuishouding'[18] fors verbeteren en heeft daarom het Rijksprogramma voor Duurzaam Digitale informatiehuishouding (RDDI) ingericht. In het Meerjarenplan is toegezegd dat de rijksonderdelen eind 2021 hun e-mails veiligstellen, websites archiveren en een groot aantal categorieën actief en beter vindbaar openbaar maken. Hier wordt nu aan gewerkt. Daarnaast wordt gewerkt aan snellere afhandeling van Wob-verzoeken, het archiveren van berichten in berichtenapps, kortere overbrengstermijnen en een campagne om medewerkers te informeren over het belang van goed informatiebeheer. Het accent van het programma verschuift van aanbod- naar meer vraaggerichte initiatieven.

De departementen hebben door nulmetingen en risico- en impactanalyses meer inzicht gekregen in hun eigen informatiehuishouding. Deze informatie en het 'Meerjarenplan verbetering informatiehuishouding' vormen de basis voor departementale plannen voor verbetering van de informatiehuishouding. In 2019 heeft het merendeel van de departementen een eigenstandig programma opgestart met verbeteracties.

Organisaties binnen de Rijksdienst delen binnen het programma RDDI actief kennis en ervaringen over informatiehuishouding met elkaar en met andere rijksorganisaties. Hierdoor kunnen interdepartementale samenwerkingsverbanden, kennisproducten, opleidingen en trainingsprogramma's, kaders en richtlijnen beter aansluiten bij de praktijk. Daarnaast wordt onderzocht of bestaande kaders door actuele ontwikkelingen vernieuwd moeten worden.

3.2 Data en artificiële intelligentie

Computers worden steeds sneller, er komt steeds meer data beschikbaar en de ontwikkelingen rondom algoritmes gaan snel. Dit zorgt voor nieuwe uitdagingen en kansen. Door data in te zetten voor uitvoering, beleid, bedrijfsvoering en toezicht worden processen niet alleen efficiënter en beter, maar ook vaak effectiever. Ministeries en zbo's innoveren nu al via innovatielabs, verkenningen naar artificiële intelligentie (AI) en samenwerkingsverbanden. Hierbij worden ook innovatieve partnerschappen met marktpartijen en wetenschap aangegaan. Daarnaast is er aandacht voor de ethische kant van data en AI. Het ministerie van BZK vervult rondom data en AI de rol van aanjager, verbinder en platform voor kennisdeling. Ook het ministerie van EZK heeft een belangrijke rol rondom data, zo heeft zij in 2019 de Nederlandse visie op datadeling tussen bedrijven[19] gepubliceerd. De ministeries van BZK, JenV en EZK hebben eind 2019 samen een brief gestuurd over artificiële intelligentie, publieke waarden en mensenrechten.[20]

Het ministerie van BZK brengt in kaart wat er binnen de Rijksdienst gebeurt en deelt actief kennis. Hierdoor ontstaat inzicht in Rijksbrede uitdagingen en kansen. Voorbeelden van uitdagingen zijn: beschikbaar maken van een goede werkplek voor data-analyses, verkrijgen

[18] *Kamerstukken II* 2018/19, 25112, nr. 4
[19] *Kamerstukken II* 2018/19, 26643, nr. 594
[20] *Kamerstukken II* 2019/20, 26643, nr. 642

van toegang tot data, vergemakkelijken van delen van data en financiering van innovaties. Voorbeelden van kansen zijn: opschalen van succesvolle initiatieven en opstellen en uitwisselen van datastrategieën.

Er wordt nader invulling gegeven aan de recent geactualiseerde Data Agenda Overheid.[21] In dit verband zal onder meer onderzoek worden gedaan naar de opkomende rol van CDO en de wijze waarop deze functie binnen het CIO-stelsel kan worden geborgd. Tevens zal Rijksbreed geïnventariseerd worden hoe vraag (datavraagstukken) en aanbod (datalabs) beter bij elkaar kunnen worden gebracht.

[21] *Kamerstukken II* 2019/20, 26643 nr. 675

4 ICT

4.1 Gemeenschappelijke voorzieningen

Om efficiënt gebruik van voorzieningen en samenwerking binnen de Rijksdienst te bevorderen, is er een aantal gemeenschappelijke ICT-voorzieningen.

- *Vernieuwen Rijksportaal*: Rijksportaal is een voorziening voor de interne communicatie en interne dienstverlening voor rijksambtenaren. In 2020 wordt een start gemaakt met de realisatie van het vernieuwde Rijksportaal;
- *Samenwerkfunctionaliteit (SWF)*: de Samenwerkfunctionaliteit ondersteunt samenwerking tussen ambtenaren onderling en met externe partijen. Uit onderzoek is gebleken dat de huidige voorziening in aangepaste hiervoor kan worden gebruikt. Dit wordt in de planperiode gerealiseerd;
- *Single-sign-on Rijk (SSOn Rijk)*: Single-sign-on Rijk is de Rijksbrede ICT-voorziening waarmee rijksmedewerkers na één keer aanmelden toegang krijgen tot toepassingen en voorzieningen. In 2020 wordt de uitgewerkte visie om te komen tot een toekomstbestendige *SSOn* binnen de Rijksdienst gerealiseerd;
- *Rijkspas*: de multifunctionele toegangspas voor Rijksgebouwen wordt doorontwikkeld om te kunnen blijven voldoen aan veiligheidseisen en wensen van gebruikers. Door gebruik te maken van dezelfde pas, dezelfde identiteiten en dezelfde processen zijn toepassingsmogelijkheden vrijwel onbeperkt uit te breiden en op grotere schaal in te zetten;
- *Rijks Identity Management (RidM)*: het Rijk Identificerend Nummer (RIN) is een uniek gegeven dat rijksambtenaren tijdens hun hele loopbaan bij het Rijk identificeert. Het normenkader voor Rijks Identificatie Management wordt in 2020 aangevuld met normen voor de dienstverleners van de centrale voorzieningen;
- *Overheidsdatacenters:* ICT-dienstverleners binnen de Rijksdienst gebruiken voor de huisvesting van hun eigen hardware (*housing*) een van de vier overheidsdatacenters (ODC's). Afgelopen jaren is een traject ingezet om het aantal overheidsdatacenters sterk te verkleinen. Dit traject zal naar verwachting in 2021 worden afgerond;
- *Enterprise Architectuur Rijk (EAR)*: de relevantie van en het benodigde onderhoud aan de Enterprise Architectuur Rijk (EAR) wordt onderzocht. De EAR moet verwijzen naar architectuurafspraken in de primaire processen van specifieke sectoren en naar de Nederlandse Overheid Referentie Architectuur (NORA). Vervolgens wordt het doel van de EAR op lange termijn bepaald.

Het ministerie van BZK maakt een plan voor het gebruik van slimme ICT-toepassingen in Rijkskantoren. Met deze ICT-toepassingen worden de werkprocessen van de medewerkers van het Rijk beter ondersteund, wordt de duurzaamheid van de gebouwen vergroot en worden facilitaire processen verder verbeterd. Als gevolg van de Covid-19 crisis is de (door)ontwikkeling en uitrol van Rijksbreed videovergaderen inmiddels versneld uitgevoerd. Daarmee wordt grootschalig thuiswerken gefaciliteerd.

Voorzieningen op het gebied van informatiebeveiliging zijn:

- *Uitbouw van het Nationaal Detectie Netwerk (NDN) bij de Rijksdienst:* het Nationaal Detectie Netwerk helpt om digitale dreigingen te detecteren. Omdat het NDN steeds effectiever is als meer partijen aansluiten, hebben ministeries afspraken gemaakt over een

versnelde uitbouw van het NDN bij de Rijksdienst. Bij tijde van schrijven zijn al 71% van alle Rijksoverheidsorganisaties op het NDN aangesloten. Gestreefd wordt om voor het eind van de planperiode van de I-agenda een volledige dekking te hebben;
- *Staatsgeheime werkplek:* er is een verkenning naar de vorm van en vereiste voor een staatsgeheime werkplek uitgevoerd. Op basis van die verkenning wordt de ontwikkeling van een dergelijke voorziening nu niet opportuun geacht, in de wetenschap dat maatwerkoplossingen per departement in dit geval de voorkeur verdienen.

De minister van BZK heeft overigens de mogelijkheid om na overleg met de departementen gemeenschappelijke voorzieningen aan te wijzen[22].

4.2 Optimale inzet van interne en externe leveranciers

De Rijksdienst maakt gebruik van de markt als dat kan, maar doet zaken zelf als het moet of beter is. De strategie voor dergelijke overwegingen wordt in de planperiode thematisch uitgewerkt. Het huidig afwegingskader wordt bijgewerkt, geconcretiseerd en in lijn gebracht met de eerder gemaakte handreiking over dit thema. Hierdoor wordt het makkelijker om het kader te gebruiken bij beslissingen over de optimale inzet van interne en externe leveranciers. Een eerder uitgevoerde verkenning naar inzet van *cloud* (publieke of commercieel aangeboden) wordt omgezet in een rijksbreed afwegingskader. Om de positie van het Rijk op het gebied van softwareontwikkeling te versterken wordt in 2020 een set van goede voorbeelden hierover gepubliceerd.

Bij de afweging over optimale inzet van interne en externe leveranciers spelen onder andere criteria een rol als (functionele) kwaliteit van software, privacy, kosten, bestaand beleid en uitgangspunten, eisen aan de informatieveiligheid en het risico van afhankelijkheid van één leverancier. Departementen voeren risicoanalyses en een *Privacy Impact Assessment* (PIA) uit voordat zij kiezen om een externe leverancier te betrekken of een aanbesteding te starten. Het risico van afhankelijkheid van één leverancier wordt altijd zo klein mogelijk gemaakt, bijvoorbeeld door inzet van open source software, en door consequent gebruik van vastgestelde open standaarden.

In 2019 is een benchmark van interne ICT-leveranciers binnen de Rijksdienst uitgevoerd op onderdelen van hun dienstverlening. De resultaten worden nu bestudeerd en zullen in 2020 tot vervolgacties leiden.

4.3 Inkoop en duurzaamheid

De Rijksdienst investeert doorlopend in de relatie met commerciële partijen en in de versterking van de ICT-inkoop. Zo is categoriemanagement en strategisch leveranciersmanagement voor een aantal grote ICT-leveranciers ingericht. Binnen de Rijksdienst worden leereffecten uit ICT-projecten gebruikt bij ICT-inkoop en -aanbestedingen. De ervaringen versterken de positie van de Rijksdienst als opdrachtgever. In 2019 is de ‘Inkoopstrategie Rijksoverheid, Inkopen met impact’ [23] opgesteld die ook van toepassing is op ICT-inkoop.

[22] *Kamerstukken II* 2018/19, 26643, nr. 573
[23] *Kamerstukken II* 2019/20, 30196, nr. 679

De duurzaamheid van ICT heeft een hoge prioriteit. In het Klimaatakkoord[24] en de inkoopstrategie van het Rijk is opgenomen dat de Rijksorganisatie in 2030 klimaatneutraal is, dat het grondstoffengebruik met 50% wordt gereduceerd, dat daarbij sociaal rendement wordt gerealiseerd en dat wordt gezorgd voor goede arbeidsomstandigheden in de productiekosten. De ICT-dienstverleners van het Rijk voeren dit uit via een ambitieuze verduurzamingsagenda ICT met vier speerpunten:

1. het voeren van een duurzame producten- en dienstencatalogus vanaf 2021;
2. te zorgen voor zoveel als mogelijk duurzame inkoop vanaf 2021;
3. het uitsluitend bezitten of gebruiken van duurzame datacenters in 2022;
4. per direct het groene en duurzame werken na te streven en de CO2-voetafdruk te minimaliseren.

Duurzaamheid wordt daarbij actief verbonden aan de andere thema's van de I-agenda. Meer inzicht in de productieketen en een zorgvuldige schoning en afdanking van apparatuur dragen bijvoorbeeld bij aan de veiligheid. Slim sturen op energie-efficiency en levensduurverlenging leiden tot lagere kosten. Ook zijn er diverse bestaande kaders die hierbij richting geven. ICT-hardware is een van tien risicocategorieën waarop de Internationale Sociale Voorwaarden[25] van toepassing zijn. Dit kader gaat over het voorkomen van misstanden in de productieketen. Energie-efficiency is een vereiste vanuit de Europese energie-efficiency richtlijn en ook het kabinetsbeleid gericht op de circulaire economie heeft invloed op de ICT van de Rijksdienst. Afgedankte ICT-apparatuur van de Rijksdienst wordt zoveel mogelijk voor hergebruik aangeboden en er wordt onderzocht hoe de levensduur verlengd kan worden. Verduurzaming van de ICT sluit aan bij de kabinetsambitie om de inkoopkracht van de overheid beter te benutten voor de duurzame transitie van Nederland en bij de kabinetsreactie op de transitieagenda's circulaire economie.

4.4 Levenscyclusmanagement

Levenscyclusmanagement is de aandacht voor de software vanaf het eerste idee tot het moment dat er afscheid van wordt genomen. Software is namelijk niet 'klaar' als een eerste versie opgeleverd is: er is beheer en doorontwikkeling nodig om te zorgen dat de software blijft werken en blijft voldoen aan de eisen vanuit bijvoorbeeld de gebruiker en rondom informatiebeveiliging. Daarnaast spelen externe factoren een rol, zoals updates van leveranciers. Maar het gaat ook om besluitvorming, financiering en innovatie. Dit betekent dat er bredere aandacht is dan alleen in de ontwikkelfase van een project. Het gaat hierbij ook om de blijvende onderhoudbaarheid van systemen en om problematische *legacy* aan te pakken en te voorkomen. In 2019 heeft de Algemene Rekenkamer hier nadrukkelijk aandacht voor gevraagd[26]. Diverse activiteiten die in deze I-agenda genoemd zijn, hebben een relatie met dit onderwerp, zoals de departementale IV-plannen die in hoofdstuk 6 beschreven worden.

Bij de (door)ontwikkeling van de informatievoorziening moet steeds een afweging worden gemaakt tussen robuustheid en flexibiliteit. Nieuwe en bestaande systemen bij de Rijksdienst worden daarom steeds vaker in kleine stappen (door)ontwikkeld. Hierdoor is er sneller resultaat, minder risico op grote fouten en ruimte voor aanpassingen waar dat nodig is. *Permanent bèta* en leren van fouten horen hierbij.

---

[24] *Kamerstukken I* 2018/19, 32813, nr. H
[25] Actieplan MVI Rijksinkoopstelsel, https://www.rijksoverheid.nl/documenten/rapporten/2017/10/24/actieplan-mvi-rijksinkoopstelsel
[26] *Kamerstukken II* 2018/19, 35200, nr. 9

Het uitgangspunt is dat er altijd een werkende, eerder gebruikte versie van een systeem inzetbaar moet zijn als een nieuwe ontwikkeling niet blijkt te werken. Dit verhoogt de veiligheid, betrouwbaarheid en bruikbaarheid van de informatievoorziening van de Rijksdienst. Deze werkwijze betekent een verandering voor medewerkers en management. Ter ondersteuning wordt een handreiking ‘beheerst vernieuwen’ ontwikkeld voor de Rijksoverheid.

5 Kennis en kunde

COVID-19 heeft het belang verder benadrukt van een overheid die ook digitaal goed functioneert. De juiste en voldoende I-capaciteit in huis is daar een essentieel onderdeel van. Voor de benodigde vernieuwing en continuïteit van de digitale dienstverlening van het Rijk moet er voldoende talent op het gebied van informatievoorziening, ICT en informatiebeveiliging aangenomen worden. Daarnaast moeten Rijksambtenaren voldoende (actuele) kennis op deze gebieden hebben. Het ministerie van BZK werkt daarom aan het versterken van i-kennis bij beleidsmakers, bevordert het aantrekken, behouden en ontwikkelen van ICT-ers en stimuleert het lerend vermogen op ICT-gebied binnen het Rijk. Bovendien wordt ingezet op het wegnemen van bestaande drempels, faciliteren en professionaliseren van ICT-werkgeverschap, vooral op het gebied van professionele (ICT) kennisontwikkeling en behoud van personeel.

5.1 Kennis en kunde binnen de I-community

Er wordt een kennisfunctie ingericht om goede voorbeelden en technologische innovaties te delen, om slagkracht en innovatie bij het Rijk een impuls te geven. Bestaande platforms, fora en expertgroepen worden beter met elkaar verbonden. Kennis en ervaringen van het BIT, van de Rijks Innovatie Community en van uitvoeringsorganisaties krijgen hierin ook een plek.

Technologische ontwikkelingen hebben grote impact op de maatschappelijke opgaven van de overheid. Om de kansen hiervan te benutten moet de Rijksdienst ontwikkelingen volgen, leren en ervaren wat nieuwe technieken betekenen en hoe zij ermee om kan gaan. Dit vraagt om structurele aandacht voor innovatie binnen de Rijksdienst, zodat zij haar taak kan blijven uitvoeren. Van zelf experimenteren leert de Rijksdienst het meest, in verbinding met elkaar, met kennisinstellingen, universiteiten en bedrijven. Het gaat dus zowel om denken als doen.

Ook de start van het I-Partnerschap, een samenwerkingsverband tussen het Hoger Onderwijs en de Rijksdienst levert een belangrijke bijdrage aan de verdere digitalisering en innovatie van de overheid. Onderdeel van dit I-partnerschap is het opzetten van innovatielabs op onderwerpen als cyber security en blockchain, waar het hoger onderwijs, Rijksorganisaties en - waar relevant - bedrijfsleven samenwerken aan maatschappelijke digitaliseringsvraagstukken van het Rijk.

5.2 Positie Rijksdienst als ICT-werkgever (HR ICT)

Om de digitaliseringsambities uit te voeren, is voldoende goede capaciteit nodig op het gebied van informatievoorziening, ICT en informatiebeveiliging (‘I-capaciteit’). Dit geldt zowel voor de ministeries, dicht bij de beleidsmakers, als voor de uitvoering. Het interdepartementale programma Versterking HR ICT Rijksdienst 2018-2021 heeft initiatieven ontwikkeld die het aantrekken, ontwikkelen en behouden van I-capaciteit, waaronder ICT’ers, bij de Rijksdienst bevorderen. Het ministerie van BZK vervult hierin de rol van aanjager, verbinder en platform voor kennisdeling.

Binnen het programma worden diverse eerder opgestarte Rijksbrede initiatieven voortgezet. Zo worden CV’s van kansrijke kandidaten met een I-profiel die aan de slag willen bij de Rijksdienst Rijksbreed gedeeld en is er een doorlopende Rijksbrede I-arbeidsmarktcampagne die zich richt op het aantrekkelijker maken van de Rijksoverheid als I-werkgever. Daarnaast wordt een verdere impuls gegeven aan het Rijks I-traineeprogramma waarin drie specialistische onderdelen zijn opgenomen, namelijk ICT, data en cybersecurity. Als gevolg van COVID-19 wordt een aantal van de initiatieven binnen het programma getemporiseerd en zal bovendien de nadruk meer worden gelegd op ontwikkeling en behoud. Hier wordt onder andere invulling aan gegeven door in te zetten op Leven Lang Ontwikkelen op I-gebied.

Ook zal de focus bij het om- en bijscholingsprogramma voor schaarse I-expertises (I-Flow) deels verschuiven naar bijscholing op I-kennis van zittend personeel.

In 2018 is gestart met het versterken van de informatiepositie over ICT-personeel, mede gebaseerd op een interdepartementale afbakening van ICT-profielen in het Kwaliteitsraamwerk Informatievoorziening. Het raamwerk biedt ook gemeenschappelijke afbakening en definities rondom ICT-personeel, wat een impuls geeft aan de samenwerking tussen departementen. Zo kan sneller en actiever ingespeeld worden op verwachte tekorten. In 2020 wordt dit raamwerk van ICT-profielen verder uitgewerkt, ook in relatie tot bijpassende opleidingstrajecten, ingevoerd als proef bij een aantal rijksorganisaties en nadrukkelijker ingezet als monitoringsinstrument.

5.3 I-bewustzijn en I-vaardigheden beleidsmakers (RADIO)

Naast het aantrekken van voldoende ICT'ers is het belangrijk dat ambtenaren in beleid, uitvoering en toezicht voldoende inzicht hebben in de mogelijkheden en effecten van digitalisering op hun werk.
Het I-bewustzijn en de I-vaardigheden van beleidsmedewerkers, project- en programmamanagers en de ambtelijke top moet worden versterkt. Ambtenaren moeten zich een onafhankelijk oordeel kunnen vormen over de toepassing van ICT in primaire- en ondersteunende processen, en een volwaardige gesprekspartner of opdrachtgever kunnen zijn voor ICT-marktpartijen. Hiervoor zullen veel rijksambtenaren moeten worden (bij)geschoold.

De Rijksacademie voor Digitalisering en Informatisering Overheid (RADIO) ontwikkelt sinds 1 oktober 2017 een aanbod om de basiskennis binnen de Rijksdienst op niveau te krijgen. Het initiatief moet komende jaren verder uitgebouwd worden. De ontwikkeling van nieuwe technologieën gaat snel en burgers en bedrijven verwachten van de overheid minimaal dezelfde digitale dienstverlening als die zij van marktpartijen ontvangen. RADIO ontwikkelt daarom een vervolgaanbod voor kennisdeling dat aansluit op de laatste ontwikkelingen. Daarbij wordt gezocht naar manieren van delen van kennis en kunde die aantrekkelijk zijn en een groot bereik hebben.

Voor deze planperiode betekent dat doorontwikkeling van het klassikale aanbod in de vorm van werksessies op nieuwe thema's. Dit sluit aan op het nieuwe digitale lesaanbod op de thema's data-gestuurd werken/data-analyse en –science/cyber security, keteninformatisering en thema's die doorlopend kunnen worden aangedragen, afhankelijk van de ontwikkelingen. Doel is om een leerplatform te ontwikkelen waarop ambtenaren de kennis over informatievoorziening kunnen vinden die ze nodig hebben.

RADIO werkt met de Algemene Bestuursdienst (ABD) ook aan het vergroten van de I-kennis en –vaardigheden van het (top)management van de Rijksdienst. Zij ontwikkelt een traject voor topmanagers bij ministeries, uitvoerings- en toezichtorganisaties.

6 Versterken van het CIO-stelsel

Informatievoorziening is tegenwoordig onlosmakelijk verbonden met beleidsdoelstellingen en beleidsuitvoering, ook in het primair proces. We noemen dit 'I in het hart van beleid'. De CIO's en hun medewerkers zijn vanuit een adviserende rol dan ook nauw betrokken bij alle initiatieven binnen hun organisatie die kansen en uitdagingen bieden voor de informatievoorziening. Dit hoofdstuk beschrijft de nieuwe instrumenten die nodig zijn voor het invullen van deze rol en om de ambities van de Rijksdienst in samenhang te realiseren. De minister van BZK kan na overleg met de departementen afgewogen rijksbrede kaders stellen[27].

6.1 Besluit CIO-stelsel Rijksdienst

Zoals aangekondigd in de Kamerbrief Beleidsreactie onderzoeken IV-governance Rijk en besluit toekomst BIT[28] wordt er een Besluit CIO-stelsel Rijksdienst opgesteld. In het Besluit CIO-stelsel Rijksdienst worden de rollen, taken, verantwoordelijkheden en bevoegdheden binnen het CIO-stelsel in samenhang gepresenteerd en geformaliseerd. Naast de departementale CIO- en CISO-functie worden de functies van de CIO Rijk en CISO Rijk en de positie van het CIO-beraad in het besluit vastgelegd. Dit besluit zal gelden voor alle onderdelen van de Rijksdienst, inclusief de agentschappen en wordt samen met het CIO-beraad uitgewerkt en vastgelegd. Het besluit zal eind 2020 worden opgeleverd en de implementatie kan in 2021 plaatsvinden.

6.2 De toekomst van het BIT

Het Kabinet heeft besloten[29] dat het Bureau ICT-Toetsing (BIT) een permanente status krijgt als onafhankelijk adviescollege, met een wettelijke grondslag. Het takenpakket van het BIT wordt verbreed. Dit wordt in 2020 in gang gezet. Daarnaast wordt het toetskader van het BIT nader geconcretiseerd en geobjectiveerd. Dit traject heeft een relatie met het Rijksbrede kwaliteitskader voor CIO-oordelen, dat in samenwerking met het CIO-Beraad zal worden ontwikkeld. Zo wordt gezorgd dat de interne ICT-beheersing en de externe onafhankelijke toetsing uitgaan van dezelfde Rijksbrede beleid- en kwaliteitskaders en vastgestelde (internationale) normen.

6.3 IV-cyclus

Het ministerie van BZK vervult haar coördinerende rol op het gebied van informatievoorziening (IV) binnen de Rijksdienst door het beschikbaar stellen van instrumenten zoals Rijksbrede kaders, richtlijnen en gemeenschappelijke voorzieningen waar deze nodig zijn. Daarnaast monitort zij de werking en naleving van deze instrumenten.

6.3.1 IV- Kwaliteitskader meerjarige departementale IV-plannen

Departementen beschrijven de kansen en consequenties van beleid op en voor informatievoorziening, ICT en informatiebeveiliging in een zogenoemd IV-plan. In 2020 werkt het CIO-beraad aan een IV-kwaliteitskader voor deze plannen. Dit ondersteunt goed opdrachtgeverschap, een goede beheersing van ICT-ontwikkeling en -onderhoud en een betere aansluiting van de departementale informatieplanning op de begrotings- en beleidscyclus.

---

[27] *Kamerstukken II* 2018/19, 26643, nr. 573
[28] *Kamerstukken II* 2019/20, 26643, nr. 656
[29] *Kamerstukken II* 2019/20, 26643, nr. 656

6.3.2 Transparantie over ICT

Op het Rijks ICT-dashboard staan alle projecten van ministeries en publiekrechtelijke zbo's met een ICT-component van tenminste €5 miljoen over de gehele looptijd van het project. Er wordt zo op uniforme wijze verantwoording afgelegd over de kosten en baten van ICT. Deze transparantie blijft belangrijk. De projecten worden door de ministeries zelf aangeleverd en bijgehouden. Het ministerie van BZK heeft hierin een coördinerende rol.

Het Rijks ICT-dashboard wordt in de planperiode stapsgewijs doorontwikkeld, waarbij wensen van de Tweede Kamer en aanbevelingen van de Algemene Rekenkamer en Auditdienst Rijk meegenomen worden. Recent heeft het Rijks ICT-dashboard een nieuwe startpagina gekregen met een verbetering van de presentatie en visualisatie van gegevens, in lijn met de Jaarrapportage Bedrijfsvoering Rijk[30]. Ook de signaleringsfunctie voor bestaande gegevens is verbeterd.

De volgende fase van de doorontwikkeling van het Rijks ICT-dashboard is inmiddels gestart. De minister van BZK heeft in 2019 het voornemen aan de Kamer gemeld om de taken, bevoegdheden en verantwoordelijkheden van departementale CIO's en het BIT te verbreden van focus op alleen ICT-projecten naar de hele levenscyclus van het hele ICT-portfolio[31]. Daarmee komen ook ICT-beheeraspecten in beeld, waardoor gewerkt kan worden aan de blijvende onderhoudbaarheid van het bestaande ICT-landschap. Deze verbreding voor de CIO en het BIT vertaalt zich ook naar de presentatie op het Rijks ICT-dashboard. Het CIO-beraad zal, in samenwerking met BIT, een voor alle partijen hanteerbare definitie voor het ICT-portfolio en de afbakening voor het BIT en Rijks ICT-dashboard formuleren.

6.3.3 CIO Flex

De hiervoor genoemde veranderingen betekenen voor de departementale CIO's en CIO Rijk een verzwaring van het takenpakket. Eind 2019 is gemeld dat het ministerie van BZK in nauwe samenwerking met UBR/I-interim Rijk een flexibele schil (CIO Flex) met hooggekwalificeerde ICT-specialisten zal realiseren [32]. In 2020 zal samen met UBR/I-Interim Rijk worden onderzocht hoe een eerste beperkte aanzet kan worden gegeven aan dit initiatief.

[30] Bijvoorbeeld Jaarrapportage Bedrijfsvoering Rijk 2018, *Kamerstukken II* 2018/19, 31490, nr. 249
[31] *Kamerstukken II* 2018/19, 26643, nr. 620
[32] *Kamerstukken II* 2019/20, 26643, nr. 656

Bijlage: Financiële paragraaf

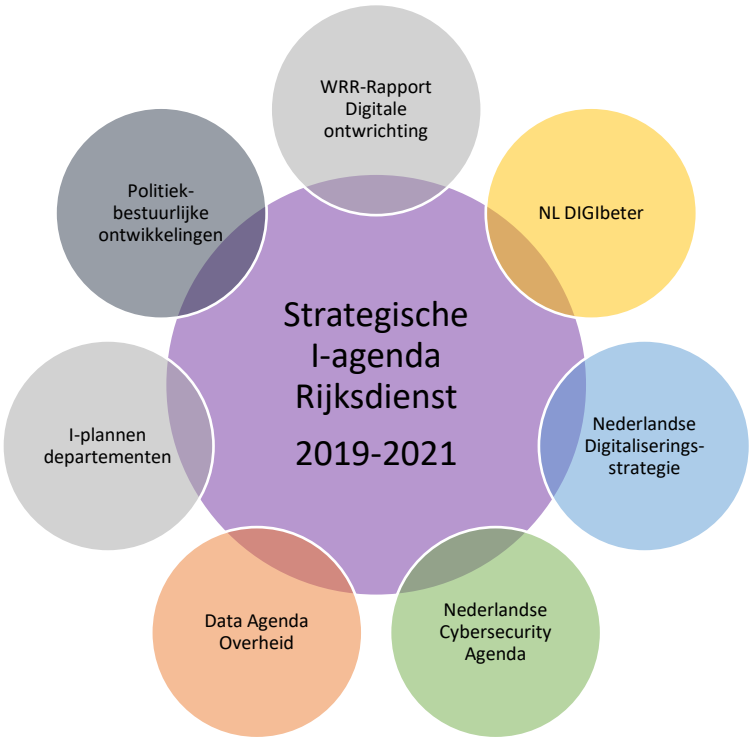
De Strategische I-agenda Rijksdienst 2019-2021 editie 2020 is ambitieus en zal ook financiële implicaties hebben. Het ministerie van BZK streeft ernaar zoveel als mogelijk de middelen binnen de eigen begroting op te vangen. Extra benodigde Rijksbrede investeringen worden op basis van een plan van aanpak inclusief dekkingsvoorstel ter besluitvorming aan de ministeries voorgelegd. Daarnaast zijn er ook de bestaande geldstromen voor gezamenlijke ontwikkeling van voorzieningen en is voor bijvoorbeeld het programma HR ICT een meerjarige bijdrage toegezegd door de ministeries. Ten slotte zullen uit deze Strategische I-agenda extra investeringen bij de ministeries voortvloeien. Deze investeringen zorgen ervoor dat de informatiehuishouding, informatiebeveiliging en de voorzieningen per ministerie op orde zijn. Ministeries dragen deze eigen kosten.

Bijlage: Context Strategische I-agenda Rijksdienst

Het kabinet-Rutte III[33] wil dat Nederland digitaal koploper wordt van Europa. Deze ambitie uit het regeerakkoord 'Vertrouwen in de toekomst' komt terug in de Nederlandse Digitaliseringsstrategie die in 2019 is herijkt[34]. Deze Nederlandse Digitaliseringsstrategie 2.0 benoemt zowel kansen als bedreigingen in de toenemende digitalisering en stelt samenwerking en verbinding centraal. Een van de ambities is "[..] Nederland als pionier en proeftuin op het gebied van verantwoorde digitale innovatie". Onder deze Nederlandse Digitaliseringsstrategie is voor en door overheden de Agenda Digitale Overheid, NL DIGIbeter[35], opgesteld. In de geactualiseerde editie uit 2019 worden vijf pijlers benoemd: innovatie, data, inclusie, digitale identiteit en regie op gegevens. In 2019 is NL DIGItaal uitgebracht, de Data Agenda Overheid[36], die in de vorige editie van NL DIGIbeter was aangekondigd. Dit document beschrijft hoe data (nog) beter kan worden ingezet voor beleid en bij het oplossen van maatschappelijke vraagstukken, met aandacht voor bescherming van publieke waarden en fundamentele rechten. Het belang van informatiebeveiliging voor de Rijksdienst werd in 2019 onderstreept in het Cybersecuritybeeld Nederland 2019[37] en het rapport 'Voorbereiden op Digitale Ontwrichting' van de Wetenschappelijke Raad voor het Regeringsbeleid[38]. Ook de Europese Unie beweegt op het gebied van digitalisering. Bijvoorbeeld: één van de zes ambities van Ursula von der Leyen, de voorzitter van de Europese Commissie, richt zich op digitalisering: *"I want Europe to strive for more by grasping the opportunities from the digital age within safe and ethical boundaries".*[39]

---

[33] Bijlage bij *Kamerstukken II* 2017/18, 34700, nr. 34
[34] Bijlage bij *Kamerstukken II* 2018/19, 26643, nr. 623
[35] *Kamerstukken II* 2018/19, 26643, nr. 621
[36] *Kamerstukken II* 2018/19, 26643, nr. 597
[37] *Kamerstukken II* 2018/19, 26643, nr. 614
[38] https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting
[39] "A Union that strives for more", Ursula von der Leyen, Political guidelines for the next European Commission 2019-2024



De Strategische I-agenda Rijksdienst staat niet op zichzelf. Deze afbeelding schetst de raakvlakken van de I-agenda met diverse richtinggevende documenten op nationaal, overheids- en rijksbreed en departementaal niveau

Bijlage: Verklarende woordenlijst en afkortingen

ABD – Algemene Bestuursdienst

AI – Artificial Intelligence

BIO – Baseline Informatiebeveiliging Overheid

BIR – Baseline Informatiebeveiliging Rijksdienst

BIT – Bureau ICT-Toetsing

CDO – Chief Data Officer

CIO – Chief Information Officer

CIO-beraad – interdepartementaal overleg van *CIO's*

CISO – Chief Information Security Officer

Cloud computing (of kortweg cloud) – een leveringsmodel om op afroep op een gemakkelijke manier via een netwerk toegang te krijgen tot een gedeelde verzameling van configureerbare ICT-componenten (bijvoorbeeld netwerken, servers, opslag, applicaties en diensten) die snel kunnen worden geleverd en vrijgegeven met minimale inspanning of interactie met leveranciers (zie ook *Public cloud*)

CTO – Chief Technology Officer

EAR – Enterprise Architectuur Rijk

FEZ - Financieel-Economische Zaken

Hosting – beschikbaar stellen van software

Housing - huisvesten van eigen hardware (buiten de eigen organisatie)

IV – informatievoorziening

Legacy – bestaande systemen met een verlengde levensduur

Levenscyclusmanagement – omvat alle aspecten die horen bij de ontwikkeling van een component van de informatievoorziening, van idee tot en met uitfasering

NDN – Nationaal Detectie Netwerk

ODC – Overheidsdatacenter

PAR – Privacy-adviseur Rijksbrede kaders en voorzieningen

Permanent bèta - werkwijze waarbij software gebruikt wordt terwijl voortdurend wordt gewerkt aan nieuwe versies met bijvoorbeeld meer functionaliteit of meer gemak

Privacy Impact Assessment (PIA) - privacy-effect-beoordeling, een gestandaardiseerd instrument om de impact van een voornemen op privacy-aspecten te kunnen bepalen

RDDI – Rijksprogramma voor Duurzaam Digitale informatiehuishouding

Single-sign-on (SSOn) – gebruikers melden zich eenmalig aan waarna zij toegang krijgen tot voorzieningen waar zij rechten op hebben, zonder dat zij zich hiervoor steeds opnieuw hoeven aan te melden

Wob – Wet openbaarheid van bestuur

Zbo – Zelfstandig bestuursorgaan