Ministerie van Justitie en Veiligheid

Departementaal Informatieplan 2024 - 2027

Managementsamenvatting

Inleiding

Het ministerie van Justitie en Veiligheid (JenV) is verantwoordelijk voor onze rechtsorde. Bovendien werken we aan een veiliger en rechtvaardiger samenleving. Daarbinnen zijn de ministers bestuurlijk verantwoordelijk voor onder meer het waarborgen van de rechtsstaat en het handhaven van de openbare orde en veiligheid, en de Staatssecretaris voor de migratie en naturalisatie. Om de maatschappelijke opgaven die hierbij horen uit te kunnen voeren, moet JenV beschikken over de juiste informatie en technologie - een solide en wendbare informatievoorziening.

Werken aan een solide en wendbare informatievoorziening, ook wel digitalisering genoemd, is werken aan verandering. Dat is de basisgedachte van de i-Strategie JenV 2022 - 2027. De samenleving verandert en haar (digitale) behoeften veranderen mee. De i-Strategie is richtinggevend en passen we waar nodig aan op basis van voortschrijdend inzicht en nieuwe opkomende ontwikkelingen. Ondertussen blijven we actueel met dit meerjarig departementaal informatieplan, dat een afgeleide is van de i-Strategie JenV 2022 - 2027. Het wordt jaarlijks geactualiseerd en naar de Tweede Kamer gestuurd.

Reikwijdte

Met dit informatieplan geven we inzicht in de grootste opgaven met een informatievoorziening (IV-)component, waar we de komende jaren voor staan. De verbinding met de i-Strategie zit in de overkoepelende activiteiten en producten die we JenV-breed realiseren voor de verschillende JenV-organisaties. Daarmee blijft de beleidsontwikkeling bij de beleids-DG-en en geven de individuele JenV-organisaties hun individuele IV-opgaven vorm in hun eigen informatieplannen.
Daar waar het ketenbrede opgaven zijn, maken we JenV-brede afspraken voor 'regie op I': kaders voor de grote, organisatie-overstijgende opgaven met een grote IV-component, zonder daarbij in de integrale verantwoordelijkheden te treden van de individuele organisaties.

Voor zowel de i-Strategie als voor dit informatieplan geldt: alle JenV organisaties gebruiken hem als kapstok voor het maken van een eigen (meerjarig) informatieplan. Zo zorgen we over alle JenV organisaties heen voor een consistent geheel.

Belangrijkste beleidsprioriteiten met een IV-component

Het veiligheidsdomein heeft verschillende beleidsterreinen met voor de komende paar jaar de nodige beleidsprioriteiten. Een flink aantal daarvan heeft ook impact op de informatievoorziening binnen het ministerie, tussen het ministerie en haar ketenpartners, en richting burgers en bedrijven. Een aantal van deze grootste opgaven staat hieronder en daarmee is het een selectie van een groter geheel aan beleidsopgaven.

Wetboek van Strafvordering
Om te zorgen voor tijdig, eerlijk en effectief recht biedt een nieuw Wetboek van Strafvordering de ruimte om nieuwe vormen van criminaliteit te bestrijden en zaken daar waar nodig en gewenst snel af te handelen. Ook zorgt het nieuwe wetboek ervoor, gelet op de razendsnelle digitale ontwikkeling van de maatschappij, dat opsporing en vervolging techniekonafhankelijk worden.
Het vernieuwen van het Wetboek van Strafvordering en de implementatie daarvan is een prioriteit van het kabinet en van het Bestuurlijk Ketenberaad voor de strafrechtketen.

Jeugd, zorg en veiligheid
De domeinen jeugd, zorg en veiligheid gaan over complexe vraagstukken die zien op diverse levensgebieden, die (inhoudelijk en technisch) onder de beleidsverantwoordelijkheid staan van meerdere ministeries. Daar zijn ook veel en uiteenlopende, publieke en private, organisaties als partner betrokken. Het is een grote uitdaging om samen structureel en zorgvuldig aan de benodigde gegevensdeling te werken, naast de aandacht voor de eigen primaire processen. In de Meerjarenagenda Zorg- en Veiligheidshuizen 2021 - 2024 ligt de basis van de ontwikkelingen in de informatievoorziening. Onder andere met het Toekomstscenario kind- en gezinsbescherming wordt ook voor jeugd aan verbeteringen gewerkt.

Migratie
Binnen de migratieketen werken we al grotendeels digitaal samen als het gaat om informatie-uitwisseling over de vreemdeling. Onder de noemer MIRA wordt op dit moment de Architectuur van de Migratieketen herijkt en toekomstbestendiger gemaakt. Daarnaast zijn er in Europees verband grote wijzigingen op komst die de informatievoorziening in het migratiedomein gaat verbreden. De komende jaren worden meerdere nieuwe Europese systemen en verordeningen geïmplementeerd met als doel Europa veiliger te maken.

Politie en Veiligheidsregio's
Het Directoraat-Generaal Politie en Veiligheidsregio's is verantwoordelijk voor een aantal belangrijke stelsels in het veiligheidsdomein: politie, brandweer, rampenbestrijding en risico- en crisisbeheersing. Een belangrijk beleidsinitiatief met een substantiële IV-component is het bevorderen van internationale samenwerking en optimalisering van (internationale) gegevensdeling vanuit het beleidsprogramma Grenzen en Veiligheid.

Artificiële Intelligentie (AI)
AI is aan een opmars bezig. Reden om het in 2020 gestarte AI-programma om te vormen naar een structurele AI-beleidsdirectie. De Europese AI-verordening die op dit moment in Brussel in onderhandeling is, reguleert AI. JenV heeft een actieve betrokkenheid bij de onderhandelingen en de verdere AI-beleidsontwikkeling. Daarnaast stimuleert JenV de verantwoorde ontwikkeling en toepassing van AI.

Autoriteit Online Terroristisch en Kinderpornografisch Materiaal
Onder de hoede van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) wordt de Autoriteit Online Terroristisch en Kinderpornografisch Materiaal - hierna de ATKM - opgericht. De basis is de Europese verordening over het tegengaan van de verspreiding van terroristisch online inhoud. Deze verordening bevat verplichtingen voor aanbieders van hostingdiensten om de verspreiding van online terroristisch materiaal tegen te gaan en dit materiaal zo nodig snel te verwijderen of te blokkeren. De ATKM, die wordt ingericht als een zelfstandig bestuursorgaan, houdt toezicht op het naleven van deze verplichtingen en kan sancties op leggen. Op termijn houdt de ATKM ook toezicht op de aanpak van de verspreiding van online kinderpornografisch materiaal. Voor de oprichting van de ATKM zijn diverse systemen nodig die bijdragen aan het opslaan en waarborgen van de privacy en overige informatievoorziening.

Ondermijning
De kerntaak van het programma Directoraat-Generaal Ondermijning is om de aanpak van georganiseerde, ondermijnende criminaliteit samen met een brede maatschappelijke coalitie naar een hoger plan te tillen. Een voorbeeld van een digitale voorziening die hierbij wordt ingezet is het Verwijzingsportaal Bankgegevens. Het vervult een belangrijke rol in de aanpak van criminele geldstromen en helpt fraude en witwassen voorkomen.

Europa
Ondertussen gebeurt er in Europa ook van alles. De komende jaren zullen meerdere verordeningen en richtlijnen in werking treden die effect hebben op de informatiehuishouding binnen het hele ministerie. Daaronder zijn de AI Verordening, de AI Aansprakelijkheidsrichtlijn, de Data Governance Verordening, de Open Data Richtlijn, de Dataverordening en de aanpassing van de eIDAS-verordening. Ook blijft onverdeelde aandacht nodig voor de juiste toepassing van de Algemene Verordening Gegevensbescherming, de AVG.

Uitvoering i-Strategie
Voortvloeiend uit de belangrijkste beleidsprioriteiten met een IV-component is er de i-Strategie JenV. De i-Strategie heeft voor de komende paar jaar acht thema's die extra aandacht krijgen. Drie ervan kregen al eerder een eigen bestuurlijk mandaat met een opdracht en budget:
- De Chief Data Officer (CDO)-agenda, ondergebracht in het i-Strategiethema 'Gegevens en algoritmes'
- Het programma Open op Orde, als onderdeel van het rijksbrede traject Open Overheid en bij JenV onder de vleugels van i-Strategiethema 'Informatiehuishouding'
- Informatiebeveiliging 2.0, als onderdeel van het i-Strategiethema 'Digitale Weerbaarheid'

In november vorig jaar werd bestuurlijk besloten tot de (uitvoering van) de i-Strategie 2022 - 2027. De i-Strategie bestaat naast de drie hierboven genoemde thema's uit vijf nieuwe thema's die in de opstartfase zitten:
- Mensgerichte dienstverlening
- I in het hart van beleid, wetgeving en uitvoering
- Versterken van de besturing van de informatievoorziening
- Doorontwikkelen van het digitaal grondvlak
- Beheerste vernieuwing

Risico's en randvoorwaarden
De grootste risico's die op dit moment spelen, gelden zeker niet alleen voor de i-Strategie, maar zijn JenV-breed van toepassing op onze hele IV-opgave. Voor het eerste risico, de uitvoerbaarheid van de opgenomen beleidsprioriteiten, is het zelfs een harde disclaimer.

Uitvoerbaarheid
De in dit informatieplan opgenomen beleidsprioriteiten zijn ambities, waarvoor in sommige gevallen de detailuitwerking nog niet klaar is en de middelen nog niet volledig zijn toegekend.
De verwachtingen in de mate waarin IV kan bijdragen aan het realiseren van de beleidsambities zijn hoog. Tegelijkertijd zijn onze inspanningen doorlopend gericht op het digitaal weerbaar blijven. De inzet op digitale weerbaarheid - en bijbehorende forse capaciteit die daarvoor nodig is - blijft een belangrijke randvoorwaarde voor het succesvol uitvoeren van onze opgaven.
Opgeteld veroorzaakt dit voor onderlinge concurrentie op de absorptiecapaciteit van de JenV-organisaties, en noopt daarmee tot het maken van keuzes in de uitvoerbaarheid. Zowel beleidsmatig als financieel.
Om aan te blijven sluiten op de behoeften vanuit de samenleving, wordt op gezette momenten in de beleids- en begrotingscyclus gekeken of de prioriteiten nog steeds voldoende in de portfolio, absorptievermogen en financiële kaders van de JenV-organisaties passen.

De indruk wekken dat het IV-domein alleen draait om de in dit informatieplan genoemde beleidsprioriteiten met een IV-component, zou een verkeerd beeld geven. Het grootste deel van het werk zit namelijk in de reguliere bezigheden: het beheer

en onderhoud - inclusief de doorontwikkeling - van het IV-landschap. Ook hierbij worden binnen het budgettair kader afwegingen gemaakt tussen beheer en onderhoud aan de ene kant, en vernieuwing aan de andere kant. Met oog voor wat een organisatie aankan qua verandering.

Absorptievermogen
Maatschappelijke en politieke verwachtingen, technische mogelijkheden en de bijbehorende veranderopgaven, en veranderingen in wet- en regelgeving zorgen ervoor dat ons absorptievermogen ver wordt overvraagd. We zullen moeten prioriteren.

Kennis en capaciteit
De arbeidsmarkt is zo overspannen dat beschikbare capaciteit - zowel kwantitatief als kwalitatief - steeds vaker een beperkende factor zal zijn voor het realiseren van de gestelde doelen. Daarnaast heeft ook JenV te maken met uitstroom van medewerkers en blijven we zoeken naar nieuwe - soms nationaal nog niet eens beschikbare - kennis voor innovatie.

Stabiele financiering
Een goede informatievoorziening ondersteunt een efficiënte en effectieve invulling van onze beleidsprioriteiten. Anders gezegd: de keuze voor investeren in IV, is ook kiezen voor een betere uitvoering van beleid. Met de vele ambities op digitalisering is zogenaamde 'stabiele financiering' een randvoorwaarde geworden voor een toekomstvaste IV.

Begroting

De benodigde budgetten voor de beleidsprioriteiten en IV-activiteiten en -producten zijn zoveel als mogelijk gedekt vanuit de reguliere middelen. Daar waar nog geen middelen beschikbaar zijn, wordt geprioriteerd, worden resultaten gefaseerd, dan wel wordt in de reguliere begrotingscyclus alsnog dekking gevraagd. Met name voor de Europese wetgevingsagenda geldt dat dekking nog een aandachtspunt is; dat betekent prioritering in de portfolio's van de individuele JenV-organisaties. Er zijn er drie soorten digitaliseringsactiviteiten te onderscheiden:

Beleidsinitiatieven die bijdragen aan grotere digitaliseringsbewegingen
Hierbij gaat het om digitaliseringsactiviteiten die voortkomen uit de beleidsprioriteiten, maar die (nog) niet strikt af te bakenen zijn in ICT-activiteiten.

Beleidsinitiatieven die leiden tot afgebakende ICT-activiteiten
Hierbij valt te denken aan vernieuwings- en vervangingsprojecten. Deze ICT-activiteiten zijn, samen met hun planning en begroting, terug te vinden op het Rijks ICT-dashboard.

JenV-overkoepelende IV-activiteiten en -producten
Deze digitaliseringsactiviteiten worden uitgevoerd onder de vlag van de i-Strategie JenV 2022 - 2027.

Inhoud

Hoofdstuk 1

Inleiding

Het ministerie van Justitie en Veiligheid (JenV) zorgt voor de rechtsstaat in Nederland, zodat mensen in vrijheid kunnen samenleven, ongeacht hun levensstijl of opvattingen. We werken aan een veilige en rechtvaardige samenleving door mensen rechtsbescherming te geven en waar nodig in te grijpen in hun leven. Soms is dat een ingrijpende maatregel, soms worden nieuwe perspectieven geopend. Altijd zijn het ingrepen die alleen JenV kan en mag doen. Recht raakt mensen.

JenV bestaat uit diverse organisaties die allemaal vanuit hun eigen taak en vanuit hun eigen wettelijk basis informatie verwerken om tot een legitieme beslissing en/of interventie komen. Steeds vaker werken we daarbij in ketens van dienstverlening waarbij samenwerking en informatie-uitwisseling tussen JenV-organisaties, met andere ministeries en met externe partijen de norm is.

Daarmee is JenV een samenwerkingsverband van organisaties die allemaal informatie verzamelen, verwerken en (met elkaar) delen. De impact van die informatie op de samenleving, op de levens van mensen, kan groot zijn. Die impact impliceert dat de organisatie en onze medewerkers een grote verantwoordelijkheid hebben in de omgang met informatie en gegevens. De verantwoordelijkheid raakt de inhoud van de informatie én de manier waarop we als ministerie dienstverlening aan burgers en bedrijven aanbieden; die is meer en meer digitaal.

1.1 Maatschappelijke opgaven als uitgangspunt

JenV is verantwoordelijk voor onze rechtsorde. Bovendien werken we aan een veiliger en rechtvaardiger samenleving. Om de maatschappelijke opgaven die hierbij horen uit te kunnen voeren, moeten we beschikken over de juiste informatie en technologie - een solide en wendbare informatievoorziening. Met dit (meerjaren) informatieplan geven we inzicht in de grootste beleidsopgaven waar we de komende jaren voor staan. En hoe we, aan de hand van prioriteiten - de acht thema's van de i-Strategie - de bijbehorende informatievoorziening van het ministerie gaan optimaliseren en verbeteren.

Want bij het succesvol kunnen blijven werken aan onze maatschappelijke opgaven hoort een volwassen en duurzame informatievoorziening. Midden in de digitale samenleving.

i-Strategie als fundament

Werken aan digitalisering is werken aan verandering. Dat is de basisgedachte van de i-Strategie JenV 2022 - 2027.[1] De samenleving verandert en haar (digitale) behoeften veranderen mee. We moeten bijvoorbeeld met elkaar digitaal (nog) weerbaarder worden, en tegelijkertijd zoveel mogelijk transparantie bieden over ons handelen. Dat brengt kansen en risico's met zich mee. Om aan de veranderende behoeften tegemoet te komen, zetten we verdere stappen om ook de uitdagingen van de toekomst aan te kunnen. Daarin maakt JenV keuzes en stellen we prioriteiten. En dat zorgt ervoor dat de i-Strategie geen overzicht is van álle ontwikkelingen op I-gebied, maar inzicht geeft in de grootste IV-uitdagingen in de komende jaren. Dat doen we langs de as van acht strategische thema's:

- Mensgerichte dienstverlening
- I-in het hart van beleid, wetgeving en uitvoering
- Versterking van de besturing van de informatievoorziening
- Doorontwikkelen digitaal grondvlak
- Digitale weerbaarheid
- Gegevens en algoritmes
- Informatiehuishouding
- Beheerste vernieuwing

De i-Strategie is richtinggevend en passen we waar nodig aan op basis van voortschrijdend inzicht en nieuwe opkomende ontwikkelingen. Ondertussen blijven we actueel met dit meerjarig departementaal informatieplan, dat een afgeleide is van de i-Strategie JenV 2022 - 2027. Het wordt jaarlijkse geactualiseerd en naar de Tweede Kamer gestuurd.

Reikwijdte

Met dit (meerjaren) informatieplan geven we inzicht in de grootste opgaven met een IV-component waar we de komende jaren voor staan. Het informatieplan biedt daarmee een selectie (en geen totaaloverzicht) van de individuele digitaliseringsopgaven van de

[1] Kamerstukken 2022/23, 26 643, nr. 935 (07 november 2022).

JenV-organisaties. De verbinding met de i-Strategie zit in de overkoepelende activiteiten en producten die we JenV-breed realiseren voor de verschillende organisaties.
Daarmee blijft de beleidsontwikkeling bij de beleids-DG-en en geven de individuele JenV-organisaties hun IV-opgaven vorm in hun eigen informatieplannen. Daar waar het ketenbrede opgaven zijn, maken we JenV-brede afspraken voor 'regie op I': kaders voor de grote, organisatie-overstijgende opgaven met een grote IV-component, zonder daarbij in de integrale verantwoordelijkheden te treden van de individuele organisaties.

Voor zowel de i-Strategie als voor dit informatieplan geldt: alle JenV-organisaties gebruiken hem - naast andere relevante beleidskaders - als kapstok voor het maken van een eigen (meerjarig) informatieplan. Zo zorgen we over alle JenV-organisaties heen voor een consistent geheel.

Binnen de (kwaliteits)kaders
In het Besluit CIO-stelsel Rijksdienst 2021 staat dat het informatieplan een strategische visie bevat over de digitalisering in het primaire proces. Daarmee legt het informatieplan een logische verbinding met de meerjarige I-strategie Rijk 2021 - 2025.[2] Naast het Besluit is het Kwaliteitskader meerjarige departementale informatieplannen van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) toegepast.

Met het informatieplan geven we ook invulling aan thema #2 'Versnellen digitale agenda' van de JenV-brede Werkagenda.[3] Tenslotte draagt het informatieplan bij aan de informatievoorziening voor de Tweede Kamer en samenleving.

1.2 Leeswijzer

Het volgende hoofdstuk benoemt een aantal grote beleidsprioriteiten van JenV voor de looptijd van de i-Strategie (vooralsnog tot 2027). 'Grote', omdat het zeker geen uitputtend overzicht is. De gekozen beleidsprioriteiten in dit informatieplan zijn aangevuld met een aantal internationale ontwikkelingen waar de JenV-organisatie rekening mee moet houden.

Daarna volgen de acht thema's van de i-Strategie JenV: de drie die al eerder met een bestuurlijk akkoord van start gingen en de vijf nieuwe thema's. Voor alle thema's wordt ook de verbinding met de thema's uit de meerjarige I-strategie van het Rijk en de Werkagenda Waardengedreven Digitaliseren gelegd.

In het laatste hoofdstuk tenslotte een aantal randvoorwaarden voor een gezonde informatievoorziening en verantwoorde digitalisering.

[2] Kamerstukken II 2020/21, 26 643, nr. 739.

[3] De Werkagenda JenV geeft opvolging aan de adviezen die voortkomen uit de kinderopvangtoeslagaffaire, onderzoekrapportages en de overheidsbrede beweging 'Werk aan Uitvoering'.

Hoofdstuk 2

Belangrijkste beleids-prioriteiten met een IV-component

Er gebeurt veel in het digitale domein. Steeds meer IV- en ICT-ontwikkelingen op zowel het ministerie zelf als daarbuiten leggen een groot beslag op de absorptiecapaciteit van de JenV-organisaties. Een aandachtspunt blijft dan ook het vinden van een werkbare focus op wat belangrijk en realiseerbaar is. Voor een gezonde werkbalans kijken we ook naar de overlap met zaken die we nu al doen, naar dingen slimmer samen doen, en naar wat gedaan moet worden vanuit Nederlandse en Europese wet- en regelgeving.

2.1 Beleidsprioriteiten

Het veiligheidsdomein heeft verschillende beleidsterreinen met voor de komende paar jaar de nodige beleidsprioriteiten. Een groot aantal daarvan heeft ook impact op de informatievoorziening binnen het ministerie, tussen het ministerie en haar ketenpartners, en richting burgers. De belangrijkste staan hieronder en daarmee is het een selectie van een groter geheel aan beleidsopgaven.

2.1.1 *Straffen en Beschermen*

Voorkomen van slachtofferschap en daderschap. Slachtoffers van criminaliteit en kwetsbare personen ondersteunen en beschermen. Daders straffen én hierbij werken aan een goede terugkeer in de samenleving voor het verminderen van de recidivebieden. Dat kunnen we niet zonder partners als gemeenten, de zorg, het sociaal domein, reclasseringsorganisaties, bedrijven en diverse anderen. Daar staat het Directoraat-Generaal Straffen en Beschermen - hierna DGSenB - voor.

Dat doen wij onder andere in de beleidsterreinen Slachtoffer-beleid, Tenuitvoerlegging strafrechtelijke beslissingen, Forensische zorg, en Jeugd, zorg en veiligheid. Op deze beleidsterreinen spelen veel IV-ontwikkelingen, hieronder de grootste van dit moment.

Slachtofferbeleid

Conform de Meerjarenagenda Slachtofferbeleid 2022 - 2025 werkt JenV aan het zo goed mogelijk uitvoeren van de slachtofferrechten en -voorzieningen die het afgelopen decennium zijn geïntroduceerd. Daarvoor zijn uiteenlopende digitaliserings-trajecten gaande, bij de verschillende betrokken organisaties. Concrete voorbeelden zijn:

- informeren en raadplegen van slachtoffers ten tijde van de tenuitvoerlegging van sancties, en de taakoverdracht daarbij van het Openbaar Ministerie naar het CJIB;
- optimalisering van MijnSlachtofferZaak voor de informatiepositie van slachtoffers;
- informatiedeling in de keten, zoals bijvoorbeeld tussen Politie en Slachtofferhulp Nederland voor Individuele Beoordeling.

Dit zijn inmiddels geplande trajecten, inclusief het inbedden in bestaande informatiesystemen en het organiseren van de benodigde samenwerking.

Tenuitvoerlegging strafrechtelijke beslissingen

Voor de tenuitvoerlegging van strafrechtelijke beslissingen werken de verantwoordelijke ketenpartners van JenV gezamenlijk aan verbeteringen. Vanwege de hoeveelheid veranderopgaven en gelimiteerde verandercapaciteit, is portfoliomanagement ingericht onder aansturing van het Coördinerend Beraad Executie (CBE), met alle relevante ketenpartners. Het CBE beslist over projecten waar minstens twee ketenpartners bij betrokken zijn, aan de hand van prioriteringscriteria en businesswaarde.

Na de invoering van de Wet herziening tenuitvoerlegging strafrechtelijke beslissingen, de wet USB, wordt onder andere in de volgende trajecten doorontwikkeld om de gegevensdeling beter digitaal te ondersteunen:
- voorlopige hechtenis;
- vrijheidsbeperkende sancties zoals toezichten door politie (gebieds- en contactverboden);
- ketenbreed op verzoek beschikbaar stellen van risicogegevens zoals medicijngebruik en gewelddadig verleden van justitiabelen;
- digitalisering executieketen: meerdere zaakstromen tussen het Centraal Justitieel Incassobureau en de Dienst Justitiële Inrichtingen - hierna DJI - van lasten tot tenuitvoerlegging.

Forensische zorg
De forensische tijdlijn - hierna FTL - is een voorziening die wordt ontwikkeld voor de professionals in de forensische zorgketen, zoals DJI en verschillende zorginstellingen. Met de FTL verbeteren we de kwaliteit van de informatie-uitwisseling en verminderen we de administratieve lasten voor deze professionals. De FTL laat, met eenmaal inloggen, gegevens zien in meerdere informatie-systemen. Bovendien worden de patiëntgegevens direct chronologisch getoond, waardoor de gebruiker snel inzicht heeft in de actuele situatie. Met de invoering van de FTL hoeven persoonsgegevens verder niet te worden gekopieerd naar de verschillende werkomgevingen van de betrokken professionals. Naar verwachting komt de FTL voor de eerste gebruikers eind 2023 beschikbaar, daarna volgt uitbreiding naar andere organisaties en doorontwikkeling.

Jeugd, zorg en veiligheid
De domeinen jeugd, zorg en veiligheid gaan over complexe vraagstukken die zien op diverse levensgebieden, die (inhoudelijk en technisch) onder de beleidsverantwoordelijkheid staan van meerdere ministeries. Daar zijn ook veel en uiteenlopende, publieke en private, organisaties als partner betrokken. Het is een grote uitdaging om samen structureel en zorgvuldig aan de benodigde gegevensdeling te werken, naast de aandacht voor de eigen primaire processen. In de Meerjarenagenda Zorg- en Veiligheidshuizen 2021 - 2024 ligt de basis van de ontwikkelingen in de informatievoorziening. Onder andere met het Toekomst-scenario kind- en gezinsbescherming wordt ook voor jeugd aan verbeteringen gewerkt.

De afgelopen jaren zijn stappen gezet in de verbetering van de informatievoorziening van partners, en de informatie-uitwisseling tussen partners onderling. De toekomstige ontwikkelingen richten zich op bouwstenen die professionals, binnen de verschillende domeinen, kunnen gebruiken. Ter ondersteuning van casusoverleg en casusregie willen we ervoor zorgen dat professionals informatie kunnen ‘verzamelen’, samen ‘analyseren’, samen ‘beslissen’ en samen ‘uitvoeren’. Er wordt in dit traject expliciet nagedacht over de rechten van betrokkenen, en over privacy en gegevensdeling.

Op dit moment worden enkele bouwstenen ontworpen, getest (vaak in pilotvorm met enkele partners) en geoptimaliseerd. Actuele voorbeelden hiervan zijn:
- generieke melding: voor het efficiënt melden van zorgen over personen, voor de Politie, Zorg- en Veiligheidshuizen, Veilig Thuis en gemeenten;
- gezagsmodule: voor het efficiënt en effectief vaststellen van familierelaties van een minderjarige, voor de Koninklijke Marechaussee, de Politie en Veilig Thuis.

2.1.2 *Rechtspleging en Rechtshandhaving*
De kerntaak van Directoraat-Generaal Rechtspleging en Rechts-handhaving - hierna DGRR - is de zorg voor de rechtsstaat. Dit is de zorg voor een vrije, veilige en rechtvaardige samenleving. Vertrouwen in de overheid is voor een belangrijk deel vertrouwen in de rechtsstaat: vertrouwen dat rechten zoals eigendom en privacy beschermd worden, conflicten en geschillen effectief en rechtvaardig worden opgelost, dat criminaliteit bestreden wordt en wetsovertreders worden berecht en burgers zich veilig voelen. Zorgen dat dit vertrouwen van de maatschappij in de rechtsstaat terecht is en behouden blijft, is een belangrijke taak van de staat die DGRR waarborgt.
Veel wetgevings- en beleidstrajecten hebben consequenties voor informatiedeling of ICT, soms kleine consequenties, soms grote. De wetgevings- en beleidstrajecten bij DGRR met de grootste ICT-impact zijn de volgende.

Nieuw Wetboek van Strafvordering
Om te zorgen voor tijdig, eerlijk en effectief recht biedt een nieuw Wetboek van Strafvordering de ruimte om nieuwe vormen van criminaliteit te bestrijden en zaken daar waar nodig en gewenst snel af te handelen. Ook zorgt het nieuwe wetboek ervoor, gelet op de razendsnelle digitale ontwikkeling van de maatschappij, dat opsporing en vervolging techniekonafhankelijk worden.
Het vernieuwen van het Wetboek van Strafvordering en de implementatie daarvan is een prioriteit van het kabinet en van het Bestuurlijk Ketenberaad voor de strafrechtketen. Het wetgevings-programma nieuw Wetboek van Strafvordering is omvangrijk en vergt dat gelijktijdig wordt gewerkt aan de verschillende wetgevings-onderdelen, aan de inventarisatie van de uitvoeringsconsequenties en de daadwerkelijke implementatie.
De grootste veranderingen met IV-consequenties van het nieuwe wetboek zijn:
- de benodigde ondersteuning in informatievoorziening als gevolg van de modernisering van opsporingsbevoegdheden;
- de veranderende positie van procesdeelnemers slachtoffer, verdachte en getuige - waarin zij stukken aan het strafdossier kunnen toevoegen en kennis kunnen nemen van stukken;
- het faciliteren van het digitaal strafproces door nieuwe regelingen - zoals het langs elektronische weg overdragen van berichten en stukken, maar ook de veranderingen als geluids- of beeldopnamen beschikbaar zijn;
- aanpassingen aan informatievoorziening ter ondersteuning van de beweging naar voren.

Stelselvernieuwing Rechtsbijstand
De overheid wil dat burgers makkelijk en snel de juiste route vinden bij een (juridisch) probleem. Daarom werken we sinds 2018 aan een toekomstbestendig stelsel van gesubsidieerde rechtsbijstand. Een stelsel waarin burgers met een (juridisch) probleem vroegtijdig, laagdrempelig en adequaat geholpen worden en waarin de rechtsbijstandverleners zo goed mogelijk hun werk kunnen doen en een vergoeding ontvangen die past bij de tijd die ze in zaken steken. Daarvoor is het programma 'Stelselvernieuwing Rechtsbijstand' vormgegeven.
Het programma loopt tot 1 januari 2026, waarna een aanpassing van de Wet op de rechtsbijstand (Wrb) volgt. De drie belangrijkste doelen van het programma zijn:

- het *voorkomen van onnodige procedures in het bestuursrecht* - zoals het voorkomen van onnodige geschillen tussen burger en overheid;
- *vroegtijdige en integrale hulp dichtbij rechtzoekenden* - zoals het verbeteren van de laagdrempelige toegang tot informatie en rechtshulp, met bijvoorbeeld een gratis 0800-nummer bij het Juridisch Loket, een belteam, een nieuwe contact center applicatie en in de toekomst ook een nieuwe website geschikt voor online dienstverlening;
- *verbetering kwaliteit dienstverlening* in het stelsel - zoals per 1 januari 2022 verbeterde vergoedingen aan rechtsbijstandverleners en de verhoogde reiskostenvergoeding per 1 juli 2023.

Naast deze doelen worden de komende jaren ICT vervangingen/ verbeteringen doorgevoerd bij het Juridisch Loket, wordt parallel het Wrb-systeem bij de Raad voor Rechtsbijstand vervangen en rekening gehouden met de benodigde ICT-flexibiliteit. Zodat toekomstige aanpassingen in de Wrb goed (eenvoudiger) in de systemen kunnen worden doorgevoerd. Een toekomstige ICT-aanpassing is gepland voor de inning van de eigen bijdrage door de Raad voor Rechtsbijstand (voorzien vanaf 1 januari 2028). Ondersteunend aan deze ontwikkelingen zijn de afgelopen jaren met betrokken stelselpartners ook tientallen pilots - waarin mogelijk ook ICT/IV-resultaten (opbrengsten) zitten - uitgevoerd.

In juni 2023 startte het Wetenschappelijk Onderzoek- en Documentatiecentrum met de overkoepelende evaluatie van deze pilots. Op basis van deze analyse wordt binnen het programma bepaald welke werkzame elementen van de pilots een plek zullen krijgen in het vernieuwde stelsel en mogelijke implementatie ervan. Met als eindresultaat een flexibel toekomstbestendig lerend stelsel dat zich continu blijft verbeteren en daardoor kan meebewegen met maatschappelijke ontwikkelingen.

Wet gegevensdeling door samenwerkingsverbanden
De Wet gegevensdeling door samenwerkingsverbanden - hierna de Wgs - is belangrijk voor de bestrijding van ondermijnende criminaliteit. Het creëert grondslagen voor multidisciplinaire gegevensdeling en maakt een einde aan de versnippering, onvolledigheid en complexiteit die nu in de praktijk worden ondervonden. Bovendien zorgt de wet voor waarborgen die in de huidige praktijk ontbreken. De Wgs regelt dat deelnemers van vier bestaande samenwerkingsverbanden straks beter gegevens kunnen delen om op hun veiligheidsterrein een volledig beeld te krijgen:

- de Zorg- en Veiligheidshuizen (ZVH's) als het gaat om bijvoorbeeld huiselijk geweld en complexe problemen met ernstig verward gedrag;
- de Regionale Informatie- en Expertisecentra (RIEC's) in de strijd tegen georganiseerde en ondermijnende criminaliteit;
- het Financieel Expertisecentrum (FEC) richt zich op de integriteit van de financiële sector en specifiek op de aanpak van illegale financiële activiteiten, terrorismefinanciering en witwassen;
- de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV) stelt rapportages op waaruit kan worden opgemaakt waar mogelijk crimineel of fiscaal ontdoken vermogen wordt verborgen.

2.1.3 *Migratie*
Het Directoraat-Generaal Migratie - kortweg DGM - staat voor een op maatschappelijk verantwoorde wijze en in overeenstemming met internationale verplichtingen gereglementeerde en beheerste toelating tot, verblijf in en vertrek uit Nederland van vreemdelingen, alsmede verkrijging van het Nederlanderschap of de intrekking daarvan. De uitvoering van de Vreemdelingenwet doen we samen met onze ketenpartners: de Immigratie- en Naturalisatiedienst (IND), het Centraal Orgaan opvang asielzoekers (COA), de Dienst Terugkeer en Vertrek (DT&V), de Politie, de Koninklijke Marechaussee (KMar), het ministerie van Buitenlandse Zaken (BZ) en de Dienst Justitiële Inrichtingen (DJI). Daarnaast zijn de gemeenten belangrijke samenwerkingspartners, zowel voor de uitvoering van de Rijkswet op het Nederlanderschap als ondersteunend op de opvang.

Binnen de Migratieketen werken we al grotendeels digitaal samen als het gaat om informatie-uitwisseling over de vreemdeling. Daarvoor werken we onder architectuur en is een Meerjarenplan Ketenvoorzieningen beschikbaar. Op dit moment wordt de Architectuur van de Migratieketen herijkt en toekomstbestendiger gemaakt (MIRA), onder andere om toekomstige ontwikkelingen beter te faciliteren.

Europese ontwikkelingen in het migratiedomein
Daarnaast zijn er in Europees verband grote wijzigingen op komst die deze informatievoor-ziening in het migratiedomein gaat verbreden. De komende jaren worden meerdere nieuwe Europese systemen en verordeningen geïmplementeerd met als doel Europa veiliger te maken. Zo krijg je als reiziger in Europa te maken met een aantal verordeningen:

- Onder het Entry - Exit systeem (EES) wordt het in- en uitreis-stempel gedigitaliseerd. Zo kunnen we voortaan direct zien of iemand te lang - dat wil zeggen langer dan de toegestane 90 van de 180 dagen - in het Schengengebied verblijft.
- Invoering van het European Travel Information and Authorization System (ETIAS) betekent dat niet-visumplichtigen, volledig digitaal een aanvraag voor een reisautorisatie naar het Schengengebied kunnen indienen. Zonder reisautorisatie mag een luchtvaartmaatschappij je niet laten instappen.

- Het Visum Informatie Systeem (VIS) wordt aangepast voor betere informatiedeling en uitgebreid met registratie van regulier verblijf voor gezinshereniging, werk of studie.
- Het Schengen Informatie Systeem (SIS) is een bestaand systeem waarin gezochte mensen en goederen worden geregistreerd. Dit systeem wordt uitgebreid met registratie van mensen die dienen te vertrekken en voor een aantal jaren niet meer binnen mogen komen.
- De Europese dactyloscopie (Eurodac) is de Europese vingerafdrukken databank. De databank wordt gebruikt om zowel in documenten als bij échte mensen de identiteit te kunnen vaststellen. Hij wordt uitgebreid met gegevens over identiteit.

Met het invoeren van deze verordeningen komt alle beschikbare informatie slim en gelijktijdig bij elkaar. Zo gaan de Schengenlanden straks op dezelfde manier om met derdelanders. Al deze systemen werken uiteindelijk samen om onderling te kunnen communiceren. Binnen Schengen worden personen correct geïdentificeerd, herkend en geregistreerd in de verschillende systemen.
Naast deze veranderingen in wetgeving wordt ook het Europees strafregister Informatiesysteem (ECRIS) aangepast. ECRIS krijgt een centrale databank (ECRIS-TCN) met informatie over burgers uit derdelanden en statelozen met een veroordeling voor ernstige feiten in één van de lidstaten.

Al deze nieuwe verordeningen en systemen werken door op het beleid en de uitvoering van de Vreemdelingenwet en vragen grote aanpassingen van de systemen van partners binnen de Migratieketen. Daarnaast worden onder andere door de KMar, de Justitiële Informatiedienst (Justid) en het DGM zelf nieuwe IV-voorzieningen gerealiseerd om deze verordeningen te kunnen implementeren.

Geïntegreerd grensbeheer
Beleidsmatig heeft Nederland een integrale visie op de toekomst van grensbeheer gerelateerd aan de in- en uitstroom van personen in Nederland. In de nieuwe Nederlandse strategie 2024 - 2029 voor geïntegreerd grensbeheer dat wordt ontwikkeld in het kader van de beleidscyclus voor Europees Geïntegreerd Grensbeheer (European Integrated Border Management, IBM), is nader uitgewerkt welke strategische keuzes Nederland maakt voor een effectief grenstoezicht. Het uitgangspunt is de volgende centrale doelstelling:

Geïntegreerd grensbeheer is een professioneel, effectief en efficiënt proces van integraal grensbeheer dat
1. maximaal bijdraagt aan de veiligheid in Nederland en het Schengengebied,
2. irreguliere migratie tegengaat, en
3. bonafide reizigers optimaal faciliteert.

Toekomstige ontwikkelingen
Naast deze bekende en vastgestelde verordeningen die moeten worden geïmplementeerd, gaan de ontwikkelingen op het migratievraagstuk snel. Zowel nationaal als internationaal (in EU-verband) worden (beleids-)voorstellen voorbereid die impact kunnen hebben op de migratieketen. Denk aan de Spreidingswet, het Europese migratiepact en de heroriëntatie op het nationale stelsel. Met impactanalyses en uitvoeringstoetsen moet worden bepaald welke impact dit heeft op de informatievoorziening in de migratieketen.

Opvang Oekraïense ontheemden

Sinds de Russische invasie in Oekraïne op 24 februari 2021 hebben al ruim 90.000 ontheemden uit Oekraïne in Nederland bescherming gezocht onder voorwaarden van de Richtlijn tijdelijke bescherming van de Europese Unie. De taak om opvang te regelen voor de ontheemden is nu via het staatsnoodrecht belegd bij de burgemeesters van Nederland en straks via de tijdelijke wet bij de colleges van B&W. Circa 75% van de ontheemden krijgt onderdak in de gemeentelijke opvang. De taak om op deze manier voor langere tijd grootschalige opvang te organiseren is nieuw voor gemeenten en Rijk.

Er is - gezien het onverwachte karakter van de invasie en de directe grote omvang van het vraagstuk - er geen noemenswaardige voorbereidingstijd geweest voor deze taak. De focus lag op het verschaffen van menswaardige opvang en een informatiebasis om in crisistijd te kunnen sturen. Dat is goed gelukt.

Nu de situatie stabiliseert en duidelijk wordt dat de gemeentelijke opvang nog zeker tot het einde van de Richtlijn Tijdelijke Bescherming (RTB[4]) + 1 jaar en mogelijk langer in stand moet blijven, is het - omwille van het nemen van de goede (bestuurlijke) maatregelen om de opvang van Oekraïense ontheemden bij de gemeenten te faciliteren - belangrijk dat JenV en de medeoverheden over meer gedetailleerde, eenduidige en actuele gegevens kunnen beschikken. De verschillende actoren in de keten (gemeenten, veiligheidsregio('s), het Knooppunt Coördinatie Informatie Oekraïne[5] en de Nationale Opvangorganisatie[6]) hebben allemaal eigen bronnen en systemen.

[4] De RTB is de Richtlijn Tijdelijke Bescherming - het EU juridische fundament onder de verblijfstitel van Oekraïense ontheemden.

[5] Het Knooppunt Coördinatie Informatie Oekraïne (KCIO) is onderdeel van het Nederlands Instituut Publieke Veiligheid.

[6] De Nationale Opvangorganisatie (NOO) is een taakorganisatie binnen het programma-Directoraat-Generaal Opvang Oekraïense Ontheemden. Deze valt onder het Directoraat-Generaal Migratie van het ministerie van JenV.

Het samenbrengen van deze informatie uit deze systemen zou moeten leiden tot het kunnen nemen van de juiste besluiten over te nemen interventies. JenV zet in op het deugdelijk organiseren hiervan in processen en systemen.

2.1.4 *Politie en Veiligheid*

Het Directoraat-Generaal Politie en Veiligheidsregio's - hierna DGPenV - is verantwoordelijk voor een aantal belangrijke stelsels in het veiligheidsdomein, namelijk: politie, brandweer, rampenbestrijding en risico- en crisisbeheersing. DGPenV creëert randvoorwaarden voor de uitvoerende organisaties om hun taken binnen deze stelsels effectief uit te kunnen voeren. Nú, en in de toekomst. Daarbij zijn goedwerkende digitale voorzieningen essentieel om binnen de kaders de vruchten te kunnen plukken van datagedreven werken, toenemende (internationale) samenwerking en gegevensdeling, en om effectief in te spelen op nieuwe vormen van (cyber)criminaliteit.

De belangrijkste beleidsinitiatieven van DGPenV met een substantiële IV-component op een rij:

- Het wetsvoorstel Wetboek van Strafvordering leidt tot relatief veel veranderingen in de strafrechtsketen in zijn geheel, maar zeker ook bij de politie in het bijzonder. Denk hierbij aan nieuwe datadefinities, aangepaste bevoegdheden en regels voor de omgang met digitale bewijsmiddelen. Deze veranderingen hebben grotendeels ook een IV-component.
- Het bevorderen van internationale samenwerking en optimalisering van (internationale) gegevensdeling leidt onder meer vanuit het beleidsprogramma Grenzen en Veiligheid tot de nodige IV-aanpassingen. Daarnaast speelt het vervangings- danwel vernieuwingsvraagstuk rondom de huidige IV-voorziening van het Korps Politie Caribisch Nederland (KPCN).
- De wet politiegegevens (Wpg) stelt regels voor de gegevens-verwerking door onder andere de politie. Omdat de Wpg al enige tijd aan herziening toe is, wordt een wetgevingstraject gestart voor de aanpassing deze wet. De belangrijkste knel-punten van de uitvoeringsorganisaties zullen worden opgelost door deze wetswijziging. Een aantal van de voorgestelde aanpassingen heeft een IV-component, bijvoorbeeld het voor de uitvoeringsorganisatie mogelijk maken om nieuwe technologieën beter te kunnen gebruiken.
- DGPenV is van een beperkt aantal systemen de systeem-eigenaar en voert zij het strategische opdrachtgeverschap. Een aantal van deze systemen (bijvoorbeeld C2000) is op afzienbare termijn toe aan vervanging danwel renovatie.
- Voor een toekomstvaste en datagedreven politiefunctie zijn additionele IV-vernieuwingsmiddelen verstrekt voor onder andere de verantwoorde toepassingen van AI en datascience, de modernisering van interceptie en het verhogen van cybersecurity.

Daarnaast lopen er beleidsvormende trajecten die in een nauwe relatie staan tot digitalisering en datagedreven werken. Zo loopt er een traject om te komen tot een ontwikkelagenda 'ter versterking van de politiefunctie' en de 'nieuwe bevoegdheden voor informatievergaring door politie voor de openbare orde en bewaken en beveiligen'. De exacte IV-voetafdruk kan pas bepaald worden na afronding van de beleidsvorming.

2.1.5 *Nationaal Coördinator Terrorismebestrijding en Veiligheid*

De Nationaal Coördinator Terrorismebestrijding en Veiligheid - hierna de NCTV - draagt bij aan een veilig en stabiel Nederland. De NCTV zet zich in voor drie maatschappelijke opgaven: contraterrorisme, cybersecurity en statelijke dreigingen. Ook zorgen ze voor het bewaken en beveiligen van objecten, personen en nationale evenementen, en voor de burgerluchtvaart. Als coördinator zorgt de NCTV voor de strategische verbinding tussen alle betrokken partners in het veiligheidsdomein, voor het reduceren van nationale veiligheidsrisico's en - als het erop aan komt - het beheersen van nationale crises.

Binnen de opgaven van contraterrorisme en cybersecurity loopt een aantal grote trajecten met een forse IV-component.

Contraterrorisme

Om de nationale veiligheid en de democratische rechtsorde te beschermen tegen terroristische en extremistisch geweld, heeft Nederland door de jaren heen een duurzame, robuuste en wendbare aanpak van terrorisme ontwikkeld. Een breed scala van partners (waaronder inlichtingen- en veiligheidsdiensten, politie, opsporingsdiensten, de justitiële keten, gemeenten, lokale professionals) zet zich in om terroristisch geweld te voorkomen. Daders van terroristische misdrijven worden opgespoord, vervolgd en bestraft, en de maatschappelijk impact van geweld wordt zo beperkt mogelijk gehouden.

Elementen van de Nederlandse aanpak van terrorisme en gewelddadig extremisme die afgelopen jaren waardevol en efficiënt bleken, moeten worden geborgd - zoals de ontwikkeling van de integrale aanpak. Juist omdat zoveel partijen een rol spelen in het voorkomen van een aanslag is de samenwerking en het uitwisselen van informatie en ervaringen van levensbelang in terrorismebestrijding.

In het kader van informatievoorziening om de aanpak te versterken zijn momenteel voor de komende jaren op twee onderwerpen ontwikkelingen voorzien:

Passenger Name Record-gegevens
De aanhoudende dreiging die uitgaat van terrorisme en ernstige criminaliteit, zoals mensenhandel en drugssmokkel, stopt niet bij de landsgrenzen. Grensoverschrijdende criminele netwerken maken gebruik van internationale reisroutes en van de mogelijkheden van het vrije verkeer van personen binnen het Schengengebied om hun criminele en terroristische activiteiten internationaal voort te zetten. Het gebruik van Passenger Name Record-gegevens draagt bij aan het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit. Zonder de reismogelijkheden van gewone passagiers te beperken. Naar aanleiding van de implementatie van de uitspraak van het Hof van Justitie van de Europese Unie over de Passenger Name Record[7] worden technische aanpassingen gedaan aan het bestaande informatiesysteem voor de verwerking van passagiersgegevens in de zo gehete Travel Information Portal[8].

Autoriteit Online Terroristisch en Kinderpornografisch Materiaal
De Autoriteit Online Terroristisch en Kinderpornografisch Materiaal - hierna de ATKM - wordt opgericht op grond van de Europese verordening voor het tegengaan van de verspreiding van terroristisch online inhoud. Deze verordening bevat verplichtingen voor aanbieders van hostingdiensten om de verspreiding van online terroristisch materiaal tegen te gaan en dit materiaal zo nodig snel te verwijderen of te blokkeren. De ATKM, die wordt ingericht als een zelfstandig bestuursorgaan, houdt toezicht op het naleven van deze verplichtingen en kan sancties op leggen. Op termijn zal de ATKM ook toezicht houden op de aanpak van de verspreiding van online kinderpornografisch materiaal. Een wetsvoorstel hiervoor is inmiddels aan de Kamer aangeboden. Voor de oprichting van de ATKM zijn diverse systemen nodig die bijdragen aan het opslaan en waarborgen van de privacy en overige informatievoorziening. De ATKM wordt op korte termijn operationeel.

Cybersecurity

Netwerk- en Informatiebeveiligingsrichtlijn 2
Als gevolg van de herziening van de Europese NIS2-richtlijn krijgen veel meer sectoren en organisaties binnen de EU te maken met wettelijke verplichtingen voor de beveiliging van hun netwerk- en informatiesystemen. Deze verplichtingen worden opgenomen in de Wet beveiliging Netwerk- en informatiesystemen, kortweg de Wbni. Als gevolg van deze wetgeving worden de taken van het Nationaal Cyber Security Centrum (NCSC) uitgebreid en worden door de herziening van de NIS2-richtlijn meer en andere organisaties aangemerkt dan nu onder de Wbni aangewezen zijn. De doelgroep van het NCSC groeit van 275 organisaties in 2018 naar 365 in 2022 naar circa 10.000 in 2024. Het NCSC moet daarom haar dienstverlening verder bestendigen en verbreden naar de hele doelgroep. Dit betekent voor het NCSC een hele andere manier van (samen)werken om de wettelijke taken te kunnen vervullen, om het - vanuit de stelselherziening - passend maken van producten en diensten.

Maar naast de implementatie van de NIS2-richtlijn is meer nodig om de digitale weerbaarheid van Nederland te verhogen. Met de implementatie van de Nederlandse Cybersecurity Strategie 2022 - 2028 (NLCS) werken we aan een digitaal veilig Nederland. Deze strategie heeft doelen en acties langs vier pijlers. Om deze doelen te kunnen bereiken wordt het stelsel voor digitale veiligheid verder versterkt. Het NCSC neemt hierin een centrale positie. Zo komt er met de integratie van het NCSC, Digital Trust Center en CSIRT-DSP[9] één Nederlandse cybersecurity organisatie. En wordt het NCSC bijvoorbeeld ook gevraagd om het bereik van het stelsel uit te breiden, actueel situationeel beeld op te stellen, en dreigings- en slachtofferinformatie waarover de overheid, bedrijven en maatschappelijke organisaties beschikken zo veel als mogelijk te ontsluiten.
Het NCSC maakt nu een uitvoeringstoets om na te gaan of het voldoende operationele slagkracht heeft om de groei van het aantal organisaties op te vangen.

Programma Cyclotron
In de periode oktober 2021 tot en met mei 2022 vond een verkenning plaats naar de mogelijkheden en randvoorwaarden om gezamenlijk sneller en gerichter informatie te delen rondom (dreigende) cyberincidenten in publiek-privaat verband. In het eindrapport wordt geadviseerd om een publiek-privaat samenwerkingsplatform op te richten, bestaande uit drie elementen: als eerste een doordeelcentrum waar snel ruwe gegevens kunnen worden gedeeld tussen hoog volwassen stakeholders, als tweede een analyse- en weerbaarheidscentrum waar gezamenlijk analyses adviezen gemaakt kunnen worden, en tenslotte een communicatie- en distributiecentrum dat zich richt op het afstemmen van de boodschap en het zorgdragen voor de distributie van informatie.

De eerste stappen in de realisatie van dit platform zijn gezet. In verschillende pilots wordt er in klein publiek-privaat verband informatie en kennis uitgewisseld. Ook is een juridische werkgroep opgericht, bestaande uit publieke en private juristen, die in kaart brengt wat er mogelijk is binnen de huidige wettelijke kaders en wat op de lange termijn wettelijk nodig is om dit platform te effectueren.

[7] HvJ EU 21 juni 2022, C-817/19, ECLI:EU:C:2022:491, (Ligue des droits humains).

[8] Zie ook Kamerstukken II, 2022/2023, 3 4861, nr. 35 en 36.

[9] Het ministerie van Economische Zaken en Klimaat richtte op 1 januari 2019 het CSIRT voor digitale dienstverleners (CSIRT-DSP) op. Meer informatie over het CSIRT-DSP is te lezen op deze website.

Op dit moment wordt verder onderzocht wat nodig is om daadwerkelijk te komen tot zo'n samenwerkingsplatform.

Doelwit- en slachtoffernotificatie (DSN)
De NLCS stelt zich tot doel dat iedereen in Nederland gewaarschuwd moet kunnen worden die (mogelijk) slachtoffer of doelwit is van een cyberaanval. Om dit te realiseren is onderzocht hoe doelwit- en slachtoffernotificatie (DSN) uit een niet-strafrechtelijke bron verder vormgegeven kan worden[10].
Er is een visie op DSN geformuleerd, waarin de Rijksoverheid een actieve rol neemt bij (de uitvoering van) DSN en waarbij nauw wordt samengewerkt met andere (private) partijen. Naar verwachting wordt eind 2023 een dienst opgeleverd die het met bestaande systemen, technisch mogelijk maakt om dreigingsinformatie te delen met organisaties die doelwit of slachtoffer zijn van een cyberdreiging. Parallel wordt gewerkt aan de verdere realisatie van een voorziening voor de langere termijn. Een voorziening die gebruik maakt van één technische oplossing, waarmee organisaties - publiek en privaat, vitaal en niet-vitaal, groot en klein, en mogelijk ook burgers - geïnformeerd kunnen worden. Zodat iedereen in Nederland beter in staat wordt gesteld de digitale weerbaarheid te vergroten. De volledige realisatie van de voorziening is voorzien voor het eerste kwartaal van 2025.

Nationaal Detectie Netwerk
In het actieplan van de NLCS staat dat alle nog niet aangesloten Rijksoverheidsorganisaties worden aangesloten op het Nationaal Detectie Netwerk. Ook wordt de samenwerking en informatiedeling tussen de partners in het NDN en de dienstverlening richting de aangesloten organisaties versterkt door onderlinge samenwerking te intensiveren.
Vanwege ontwikkelingen in het detectielandschap zal het huidige NDN op termijn waarschijnlijk zijn meerwaarde verliezen. Omdat het onverminderd nodig blijft om voldoende zicht te houden op de digitale dreiging onderzoeken we nu wat nodig is om een toekomstbestendig detectiestelsel in te richten.

2.1.6 *Ondermijning*
De kerntaak van het programma Directoraat-Generaal Ondermijning - hierna DGO - is om de aanpak van georganiseerde, ondermijnende criminaliteit samen met een brede maatschappelijke coalitie naar een hoger plan te tillen. In de afgelopen jaren is samen met private en publieke partners gebouwd aan het fundament van de integrale aanpak van georganiseerde criminaliteit. Die integrale aanpak richt zich van lokaal tot internationaal niveau op dezelfde prioriteiten: voorkomen dat kwetsbare jongeren de criminaliteit worden ingezogen door in te zetten op preventie met gezag, verstoren van het verdienmodel/doorbreken van criminele netwerken, opsporen en bestraffen van zware criminelen, en het beschermen van de personen die dagelijks in de frontlinie van de aanpak staan, zoals politiemensen, officieren van justitie, burgemeesters en journalisten.

Om de aanpak van georganiseerde criminaliteit duurzaam te versterken, zijn er de afgelopen jaren op verschillende momenten middelen beschikbaar gesteld. Zo zijn er met de ontwerpbegroting 2022 incidentele gelden beschikbaar gesteld die prioritair zijn ingezet voor problematiek in de informatievoorziening. Door te investeren in het stap voor stap opruimen en moderniseren van verouderde informatievoorziening - de zogeheten IV-legacy - is de basis van de ondermijningsaanpak in orde. Hiermee worden problemen bij partnerorganisaties op het gebied van beheersbaarheid en beveiliging aangepakt en wordt bijgedragen aan beleidsinitiatieven binnen de integrale aanpak. Dit ondersteunt ook de samenwerking in de strafrechtketen en voorkomt kwetsbare systemen.

Binnen de integrale aanpak is DGO geen systeemeigenaar van IV-systemen. Wel is er een aantal beleidsinitiatieven van DGO die een substantiële IV-component hebben en zijn er digitale voorzieningen waarvan DGO het strategische opdrachtgeverschap voert danwel middelen voor beschikbaar heeft gesteld.
Voorbeelden van digitale voorzieningen zijn de UBO-registers[11] en het Verwijzingsportaal Bankgegevens. Beide voorzieningen vervullen een belangrijke rol in de aanpak van criminele geldstromen - ze helpen fraude en witwassen voorkomen. Ook binnen andere deelopgaven is er vaak sprake van een IV-component, maar is die veelal ondersteunend aan het betreffende beleidsinitiatief en vormt het niet de kern van het initiatief zelf. Dit geldt bijvoorbeeld voor de Forensische Opsporing, waarbij is geïnvesteerd in de IV-systemen van de strafrechtketenpartners voor de borging van onderzoekskwaliteit binnen het forensisch werkveld, en de investeringen binnen het RIEC-LIEC bestel voor de regionale versterking.

2.1.7 *Ketenontwikkelingen*
Duurzaam Digitaal Stelsel Strafrechtketen
Sinds 1 januari 2023 wordt de samenwerking binnen de strafrechtketen voor de informatievoorziening (IV)-opgave vormgegeven in het Duurzaam Digitaal Stelsel (DDS). Met het realiseren van het DDS wordt de digitalisering in de strafrechtketen structureel georganiseerd, bemenst en bekostigd. Het verbeteren van de informatie-uitwisseling tussen de ketenpartners in de strafrechtketen staat hierbij centraal. Het DDS draagt door het stap voor stap verder digitaliseren van de strafrechtketen bij aan een

[10] Informatie over doelwitten en slachtoffers kan zowel uit strafrechtelijke als niet-strafrechtelijke bron komen. Er gelden verschillende juridische regimes om deze informatie vervolgens te verwerken en daarnaast zijn er andere partners betrokken bij de verschillende trajecten. Conform het NLCS Actieplan, komt er een aparte verkenning voor het notificeren van slachtoffers uit strafrechtelijke bron. De ambitie is om deze twee trajecten in de toekomst met elkaar te integreren.

[11] In het UBO-register staan alle 'Ultimate Beneficial Owners' of 'uiteindelijk begunstigden' van een vennootschap of juridische entiteit geregistreerd. Het doel van het register is verdere bestrijding van witwaspraktijken en andere economische criminaliteit.

geoptimaliseerde strafrechtspleging, een betere dienstverlening aan de burger en een betere ondersteuning van de professional die in de keten werkzaam is. Binnen het DDS werkt de strafrechtketen samen verder aan een steeds betere informatie-uitwisseling binnen de keten, bijvoorbeeld met de uitwisseling van multimedia. De komende jaren hebben de IV-ontwikkelingen die nodig zijn voor de invoering van het nieuwe Wetboek van Strafvordering prioriteit.

2.2 Ontwikkelingen internationaal

Samenwerken in en rondom Europa klinkt logisch, maar is nog steeds niet overal vanzelfsprekend. Europa is bij uitstek een speelveld waar samenwerking veel meerwaarde kan opleveren. Want wij mogen dan nog wel fysieke grenzen hanteren, in de digitale wereld gelden die al lang niet meer.
Het is dan ook niet voor niets dat de Europese Commissie het Digitaal Kompas heeft gelanceerd: vier concrete actieterreinen voor de komende tien jaar:

- een digitaal vaardige bevolking en hooggekwalificeerde digitale professionals;
- beveiligde, goed presterende en duurzame digitale infrastructuurvoorzieningen;
- de digitale transformatie van bedrijven;
- de digitalisering van overheidsdiensten.

Ook werken we op Europees niveau samen aan het versterken van onze digitale concurrentiekracht in een geglobaliseerde wereld. Bijvoorbeeld rondom AI-ontwikkelingen, met afspraken over de bescherming van de privacy van onze burgers, en het makkelijker kunnen inzetten van IV- en ICT-expertise uit andere (Europese) landen. Daar hoort ook de nodige Europese regelgeving bij.

De komende jaren treden meerdere Europese verordeningen en richtlijnen in werking die gevolgen hebben voor de informatie-huishouding binnen het rechtsbestel. Daaronder zijn de AI Verordening[12], de AI Aansprakelijkheidsrichtlijn[13], de Data Governance Verordening[14], de Open Data Richtlijn[15], de Dataverordening[16] en de aanpassing van de eIDAS-verordening[17].

Het inpassen in de bestaande begrotingen van de financiële dekking die nodig is voor de implementatie van deze verordeningen noopt tot prioriteren.

Daarnaast blijft ook onverdeelde aandacht nodig voor de juiste toepassing van de Algemene Verordening Gegevensbescherming, de AVG.

Parallel hieraan zet de EU stappen naar digitalisering van grens-overschrijdende justitiële samenwerking. De bewijsverkrijgings-verordening en de betekeningsverordening zijn een eerste stap en worden al geïmplementeerd. De Verordening en de richtlijn digitalisering justitiële samenwerking en toegang tot het recht[18] - bekend onder de naam eJustice - treden naar verwachting nog dit jaar in werking; ze worden de komende jaren stapsgewijs geïmplementeerd. Naast deze verordening en richtlijn richten de Europese initiatieven zich op de digitale samenwerking en informatie-uitwisseling rond terrorisme en de zogenoemde Joint Investigation Teams (JITs)[19].

2.3 Verbinding met overkoepelende IV

De verbinding van de belangrijkste beleidsontwikkelingen uit de vorige paragrafen met de i-Strategie zit hem in de i. De i-Strategie richt zich - langs de lijn van de acht inhoudelijke thema's - op de overkoepelende IV-activiteiten en -producten. Denk aan kaders, voorzieningen en leer- en samenwerkingsinitiatieven die meerwaarde bieden aan de individuele organisaties met hun eigen informatieplannen, en ondersteunend zijn aan de vaak ketenbrede beleidsopgaven.

Bijvoorbeeld bij de herziening van het Wetboek van Strafvordering. In het wetboek staan de regels voor de opsporing, vervolging en berechting van strafbare feiten en voor de tenuitvoerlegging van opgelegde straffen. Regels waar de Politie, het Openbaar Ministerie, rechters en advocaten zich aan moeten houden.
Het nieuwe wetboek helpt de strafrecht-keten optimaal te functioneren en sluit beter aan bij de aanpak van nieuwe vormen van misdaad, zoals digitale criminaliteit. Daar komen thema's als 'digitale weerbaarheid' en 'gegevens en algoritmes' direct om de hoek kijken.
Daarnaast moet ook de informatie in de (keten)systemen erachter op orde zijn (informatiehuishouding), en moeten de systemen voldoen aan dezelfde standaarden om naadloos met elkaar te kunnen communiceren (digitaal grondvlak) zonder dat informatie ergens blijft hangen. En als de systemen moeten worden vervangen om mee te kunnen blijven bewegen met verbeterde processen (beheerste vernieuwing), is het wel zo handig om van tevoren na te denken over de informatie die aan het einde van het proces nodig is (I in het hart).

[12] De achtergrond(en) bij de AI-verordening.
[13] De tekst van de AI-aansprakelijkheidsrichtlijn.
[14] Uitleg van het Kenniscentrum Europa Decentraal over de Data Governance Verordening.
[15] Uitleg van het Kenniscentrum Europa Decentraal over de Open Data Richtlijn.
[16] De achtergrond(en) bij de Dataverordening.
[17] Uitleg van het kenniscentrum Europa Decentraal over de eIDAS-verordening.
[18] Meer informatie over de Verordening en richtlijn digitalisering justitiële samenwerking en toegang tot het recht.
[19] Een Eurojust-filmpje van 4 minuten met uitleg over Joint Investigation Teams.

Hoofdstuk 3

Uitvoering i-Strategie

De i-Strategie JenV bestaat uit acht thema's. Drie ervan kregen al eerder een eigen bestuurlijk mandaat met een opdracht en budget:
- de Chief Data Officer (CDO)-agenda, ondergebracht in het i-Strategiethema 'Gegevens en algoritmes';
- het programma Open op Orde, als onderdeel van het rijksbrede traject Open Overheid en bij JenV onder de vleugels van i-Strategiethema 'Informatiehuishouding';
- het programma Informatiebeveiliging 2.0, als onderdeel van het i-Strategiethema 'Digitale Weerbaarheid'.

Ook werd in november vorig jaar bestuurlijk besloten tot de (uitvoering van) de i-Strategie 2022 - 2027. De i-Strategie bestaat naast de drie hierboven genoemde thema's uit vijf nieuwe thema's die in de opstartfase zitten. Uiterlijk in 2024 ronden we de opstartfases af en houden we alle acht thema's opnieuw tegen het licht. Dit kan leiden tot andere prioriteiten, het aanpassen van de reikwijdte van een of meer thema's of het opnemen van nieuwe thema's.

In de volgende paragrafen komen de acht thema's gedetailleerder aan bod met een terug- en vooruitblik. Ook is voor elk van de thema's aangegeven aan welke onderdelen van de Werkagenda Waardengedreven Digitaliseren en de I-strategie Rijk 2021 - 2025 zij bijdragen.

3.1 Gegevens en algoritmes

Dit thema startte onder de noemer 'datagedreven werken'. In lijn met de I-strategie Rijk en de ontwikkelingen binnen ons ministerie is gekozen voor het hernoemen naar 'gegevens en algoritmes'.

Het werken met gegevens moet een organisatorische vaardigheid worden binnen JenV. Hiervoor is verdere verkenning en uitwerking nodig van vier beleidsterreinen:
Gegevenstypering (eenheid van taal), gegevenskwaliteit, gegevens-deling en gegevens-gebruik. Ze worden verder uitgewerkt via de Chief Data Officer (CDO)-agenda van de komende jaren.
Deze uitwerking bestaat uit het opstellen van concreet beleid in de vorm van sturende aanwijzingen en hierop gebaseerde hulpmiddelen zoals afspraken, modelovereenkomsten en procesafspraken. Met het JenV Datalab lossen we samen met andere JenV-organisaties concrete organisatievraagstukken op. Daarmee innoveren we steeds verder, onder andere op het gebied van AI, Privacy Enhancing Technologies (PET), en Natural Language Processing (NLP). Daarnaast wordt het JenV Datalab aankomend jaar omgevormd tot een gemeenschappelijke dienst.

Het i-Strategiethema 'Gegevens en algoritmes' wordt ingekleurd met de CDO-agenda. Daarbij staat het governancestelsel rondom gegevens nog in de kinderschoenen, zowel bij JenV als interdepartementaal en interbestuurlijk. Een consolidatie, formalisering en concretisering van dit stelsel is gaande en krijgt de komende jaren zijn beslag in zowel het (aangepaste) Besluit CIO-stelsel Rijksdienst als vanuit de beleidslijnen. De gevoelde urgentie - gezien de vele maatschappelijke en rijksbrede ontwikkelingen, kansen en risico's op het gebied van gegevens - is groot en vraagt hier ook om.

Beoogde resultaten
In de CDO-agenda staat wat en op welke manier we dingen bereiken. Hieronder een puntsgewijze samenvatting:
1. De vier gegevensbeleidsterreinen worden concreet ingevuld op basis van casuïstiek en bestaande best practices bij JenV-onderdelen. Dat gaat resulteren in een JenV Afsprakenstelsel Gegevens (JAG). Daarmee sluiten we aan bij het federatieve datastelsel van de interbestuurlijke datastrategie (gegevensdeling als een organisatorische vaardigheid) en de gegevensboekhouding.
2. Voor gegevensknooppunten worden stappen gemaakt om voor de beleidsdirecties gegevensdiensten aan te bieden waarmee ze gegevens kunnen verwerken voor evidence based beleidswerk, sturing, effectmeting en verantwoording.
3. JenV werkt aan (de doorontwikkeling van) algoritmeregisters en het bij elkaar brengen van ontwikkelingen rondom ethische dilemma's in gegevensgebruik en gegevensdeling.
4. We delen kennis door onder andere een specialistische conferentie voor alle JenV-onderdelen op het gebied van kennis-, informatie- en datamodelleren, webinars gebaseerd op thema's uit de CDO-agenda, en het leveren van relevante content op de datacommunity.
5. Voor haar onderdelen biedt JenV opleidingen op het gebied van gegevensstrategie, gegevensmanagement, gegevensarchitectuur en gegevensgovernance. Ook specialistische modules zoals wetsanalyse en gegevensleveringsprotocol worden aangeboden.

6. Er wordt een start gemaakt met gegevensbeginselen en een architectuurvisie gegevenshuishouding waar aansluiting wordt gezocht met de *European Dataspaces* - dat gebeurt onder andere in samenwerking met TNO. Ook werken we een dataradar die de duiding en impact van gegevensgerelateerde wetgeving inkleurt, verder uit.

Inzet op gegevensdeling versterkt
Om gegevensdeling te versnellen en toekomstbestendig te maken, richt JenV een tijdelijke 'Taskforce Gegevensdeling' op. Deze taskforce richt zich op het aanpakken van knelpunten in gegevensdeling op gebieden zoals de georganiseerde en ondermijnende criminaliteit, maar ook op problemen bij gegevensuitwisseling met instanties zoals het UWV en de Belastingdienst. De taskforce heeft drie hoofdtaken:

a. Het bieden van directe ondersteuning aan beleidsdirecties bij het aanpakken van gegevensdelingsvraagstukken; met een flexibele, samenwerkingsgerichte en adaptieve aanpak.
b. Het uitvoeren van gedegen analyses om de onderliggende patronen van gegevensdelingsknelpunten bloot te leggen, met als doel bij te dragen aan systeemoplossingen binnen JenV, inclusief het versterken van de JenV innovatiekracht.
c. Het ontwikkelen van richtlijnen, best practices en kaders voor gegevensdeling; altijd met aandacht voor relevante wet- en regelgeving en privacybescherming, in nauwe samenwerking met andere JenV-teams en externe partners.

Eenheid van taal
Gegevensdeling en gebruik staat of valt met de mate waarin 'eenheid van taal' in de digitale systemen van de overheid wordt bereikt. Dat begint bij het schrijven van wetten en/of het formuleren van beleid en eindigt bij de realisatie van gegevens-structuren en regelspecificaties binnen de informatievoorziening.

Artificiële Intelligentie

Artificiële Intelligentie (AI) is bezig aan een opmars. Net als in de rest van de samenleving zijn er ook bij JenV aanmerkelijke baten te verwachten bij de verantwoorde toepassing van AI. Maar ook bij de aanpak van de veiligheidsrisico's van AI (zie ook cybersecurity) en de rechtsbescherming van burgers tegen slechte AI heeft JenV een rol. Daarom is het in 2020 gestarte programma Artificiële Intelligentie eind 2022 omgevormd tot een structurele AI-beleidsdirectie. Gegevens zijn de brandstof voor artificiële intelligentie. De activiteiten van het CDO-office en de AI-directie worden daarom nog nauwer met elkaar verbonden.

Het i-Strategiethema 'Gegevens en algoritmes' representeert die verbinding. Prioritair daarbij zijn: het versterken van transparantie door het opzetten van algoritmeregisters in het JenV-domein, het stimuleren van de verantwoorde ontwikkeling en toepassing van AI-tools, en het van borgen van de ethische verantwoorde inzet van AI en algoritmen door JenV voor te bereiden op de komst de Europese AI-verordening.

Verbinding met de andere digitale thema's

Digitale agenda	(draagt bij aan) thema	
i-Strategie JenV 2022 - 2027	# 2	I in het hart
	# 4	Digitaal grondvlak
	# 5	Gegevens en algoritmes
	# 6	Informatiehuishouding
I-strategie Rijk 2021 - 2025	# 6	Naar data en algoritmen met waarde(n)
Werkagenda Waardengedreven Digitaliseren	§ 1.4	(EU) regelgeving en implementatie in samenhang ondersteunen
	§ 2.1	Publieke waarden borgen
	§ 2.2	Borgen van privacy, verantwoord datagebruik en vergroten transparantie over gegevensverwerking en -deling
	§ 3.1	Regie op gegevens
	§ 3.3	Algoritmes reguleren
	§ 4.2	Meer waarde voor specifieke burgers en organisaties, en betere beleidskeuzes met hoge datakwaliteit door adequate data-architectuur, -systemen en -richtlijnen

3.2 Informatiehuishouding

Het rijksbrede actieplan Open op Orde en de Wet open overheid (de Woo) blijven in ieder geval tot 2026 binnen Informatiehuishouding de dominante onderwerpen.
Daarnaast heeft het kabinet een wetsvoorstel ingediend voor een nieuwe Archiefwet 2021 die mogelijk in 2024 wordt ingevoerd. De belangrijkste verandering is dat overheidsarchieven na 10 jaar worden overgebracht en openbaar worden gemaakt. Omdat JenV met veel persoonsgegevens werkt, is de impact groot. Daarom wordt ook gekeken naar alternatieve oplossingen om de privacy en zorgvuldigheid te waarborgen, wellicht in de vorm van JenV-specifieke regelgeving.
Ook doet JenV vanaf 2023 mee aan een pilot onder regie van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De pilot moet leiden tot een voorgeschreven manier voor het veiligstellen van chatberichten; eerst voor de pilotdoelgroep en daarna ook voor sleutelfunctionarissen van het ministerie.

Streefbeeld
Voor het zijn van een transparante en verantwoordelijke overheid,
1. die in staat is om haar taken effectief uit te voeren,
2. die hierover verantwoording kan afleggen aan het parlement, en
3. antwoord kan geven op vragen van burgers en andere belanghebbenden kunnen we niet zonder een goede informatiehuishouding.

De 'Beleidsvisie informatiehuishouding en transparantie' beschrijft de veranderkoers van de informatiehuishouding (hierna: IHH) van JenV die nodig is om de doelen van IHH beter en blijvend te ondersteunen. Daarnaast is het een handvat voor het afwegen, selecteren en prioriteren van de meest waardevolle werkzaamheden gericht op het realiseren van die doelen. De beleidsvisie maakt inzichtelijk op welke speerpunten we op korte en middellange termijn sturen en waaraan projecten en programma's op het gebied van IHH en transparantie (zoals Open op Orde) ondersteunend zijn. Eind 2023 is het streefbeeld klaar, waarna het JenV-programma Open op Orde er op aansluit.

Open op Orde
In de kabinetsreactie op het rapport 'Ongekend onrecht' heeft het kabinet onder andere maatregelen aangekondigd voor actieve openbaarmaking van informatie en op verbetering van de informatiehuishouding bij de ministeries ('Open op Orde'). Verder schrijft artikel 3.5 van de Woo voor dat een bestuursorgaan in de jaarlijkse begroting aandacht besteedt aan de beleidsvoornemens voor de uitvoering van de Woo en in de jaarlijkse verantwoording verslag doet van de uitvoering ervan (de openbaarheidsparagraaf). Het doel van de Woo is een open overheid, die zorgdraagt voor een adequate en toegankelijke informatievoorziening op basis van een ordentelijke informatiehuishouding.

In 2021 startte JenV met de planvorming en eerste realisatie binnen Open op Orde. De uitdagingen op het vlak van informatiehuishouding binnen JenV zijn omvangrijk en divers. Ze zijn over een periode van jaren ontstaan, onder meer door een explosieve groei van data en informatie, het sterk toegenomen gebruik ervan, personele krapte en complexe wet- en beleidsstelsels die met deze informatie uitgevoerd en ondersteund moeten worden.
De veelheid en verscheidenheid aan deelnemende JenV-onderdelen en organisaties - die ook nauw samenwerken en onderlinge afhankelijkheden kennen in de verschillende ketens van JenV - maken het tot een zeer uitdagend geheel. De kabinetsdoelstellingen voor de verbetering van de informatiehuishouding zijn terecht en begrijpelijk ambitieus. Daarbij zijn realistische verwachtingen qua tempo van de realisatie versus geformuleerde ambities een belangrijk aandachtspunt.
Om de veranderopgave te kunnen managen, is een programma ingericht met een meerjarig portfolio. Het portfolio is opgebouwd langs de vier actielijnen van Open Op Orde en ingedeeld in categorieën: de rijksbrede prioriteiten en drie JenV prioriteiten: digitalisering van werkprocessen, verbeteren van gegevenskwaliteit in de ketens en papier uit de ketens.

Beoogde resultaten
Het programma Open op Orde werkt met en voor de verschillende JenV-organisaties, in de periode tot en met 2026, aan de noodzakelijke verbetering van:
1. Verbeterde duurzame toegankelijkheid: aanwezige en gebruikte gegevens (inclusief documenten en content) blijven leesbaar en in de oorspronkelijke vorm beschikbaar totdat de wettelijke termijn verlopen is.
2. Verbeterde traceerbaarheid van processtappen: de manier waarop een resultaat tot stand is gebracht, is te construeren op basis van de doorlopen stappen die tot dit resultaat hebben geleid.
3. Vergrote betrouwbaarheid van gegevens: het op een juiste manier kunnen duiden van de waarde (data) van een gegeven (betekenis) in termen van betekenis, authentiek, controleerbaar, correcte substitutie.
4. Vergrote kenbaarheid van de datacontext: het interpreten van de juiste context van de beschikbare data (waardes) - de transitie van 'data' naar 'informatie'; om juist gebruik van data te verhogen is het nodig om de betekenis en de context te weten waarin de data is ontstaan.
5. Verbeterde beschikbaarheid en juiste IHH-kennis en kunde: de vaardigheden van medewerkers vormen een belangrijke component om het gestelde doel te behalen; zowel in termen van communicatie met de maatschappelijke doelgroepen als het beheren en (door)ontwikkelen van de benodigde oplossingen.

Openbaarmaking
Binnen het ministerie is de directie Openbaarmaking in oprichting. Als eerste prioriteit is een verbeterde aanpak van de passieve openbaarmaking opgepakt - het afhandelen van Woo-verzoeken. Daarnaast voert de nieuwe directie twee verkenningen uit: de eerste naar de ondersteuning van parlementaire onderzoeks-commissies en de tweede naar actieve openbaarmaking. Deze organisatorische ontwikkeling raakt aan het beheer van onze informatie en daarmee ook aan het CIO-stelsel.

Verbinding met de andere digitale thema's

Digitale agenda	(draagt bij aan) thema	
i-Strategie JenV 2022 - 2027	# 6	Informatiehuishouding
I-strategie Rijk 2021 - 2025	# 5	Informatiehuishouding
Werkagenda Waardengedreven Digitaliseren	§ 4.1	Overheidsinformatie is duurzaam toegankelijk voor openbaarmaking

3.3 Digitale weerbaarheid

Het doel van dit thema is het verhogen van de digitale weerbaarheid van het ministerie, zodat de kloof tussen de digitale dreigingen en digitale weerbaarheid kleiner wordt. Omdat de digitale weerbaarheid van het hele ministerie als totaal afhankelijk is van de digitale weerbaarheid van haar onderdelen, richt het thema zich op de laatste: de JenV-organisaties als de som der delen. Het motto is dat elke organisatie verantwoordelijk is voor de eigen digitale weerbaarheid en dat alle organisaties mede-verantwoordelijk zijn voor de digitale weerbaarheid van het ministerie.

Met het oog op duurzaamheid wordt samengewerkt met het gelijknamige tweede thema van de I-strategie Rijk 2021 - 2025; de CIO JenV is rijksbreed portefeuillehouder van dit thema. Juist op digitale weerbaarheid is het belangrijk om maatregelen niet solistisch te treffen, maar over de grenzen van de organisatie en het ministerie heen te kijken. Dit geldt ook voor (de implementatie van) beleid en wetgeving vanuit Europa, zoals de NIS2-richtlijn. Cyberaanvallen vinden plaats daar waar de cyberweerbaarheid het laagst is.

De beoogde resultaten van dit thema gaan over het identificeren, voorkomen, detecteren, reageren en herstellen van gebeurtenissen op het gebied van digitale weerbaarheid. De aandacht van de resultaten verschuift daarbij van het ontwikkelen van beleid en het controleren van de naleving daarvan, naar het uitvoeren van het beleid van het beleid. Anders gezegd: de beoogde resultaten richten zich op de feitelijke digitale weerbaarheid.

Beoogde resultaten
De centrale resultaten worden gehaald onder de vlag van het 'programma Informatiebeveiliging 2.0 (IB2.0)'. De organisaties van het ministerie staan aan de lat om met die centrale resultaten hun eigen, decentrale resultaten te halen. Die centrale en decentrale resultaten richten zich op het automatiseren van de informatiebeveiligings-processen. Zo vergroten we de digitale weerbaarheid van het ministerie als geheel.

- Weerbaar personeel
  Dit aspect richt zich op het herkennen en behandelen van risico's door collega's, zoals de omgang met e-mail, SMS- en Whatsapp-berichten en gerubriceerde informatie. Ook leren en oefenen zij de gedragsregels op het gebied van informatiebeveiliging. Menselijke handelingen zoals het klikken op links in zakelijke e-mail, zijn vaak de eerste stap in cyberaanvallen.
  De producten en -diensten die we hierbij gebruiken:
  - E-mail en SMS phishing simulaties
  - Opleidingen

- Toegangsbeveiliging
  Hierbij is de aandacht expliciet gericht op het beheer van accounts met hoge rechten, zoals accounts van beheerders. Het misbruik van slecht beveiligde accounts met hoge rechten is vaak een volgende stap in cyberaanvallen.
  De digitale dienst die we hiervoor inzetten:
  - Toegangsbeveiliging voor beheerders

- Beveiligingsbedrijfsvoering
  Om malware besmettingen te helpen voorkomen, richt dit aspect zich op het beheren van technische activa, kwetsbaarheden, configuraties en werkplekken.
  De digitale diensten die we hiervoor inzetten:
  - Beheer kwetsbaarheden en technische configuraties
  - Inventarisatie technische componenten
  - Software 'bill of materials'

- Communicatiebeveiliging
  Onder deze noemer treffen we maatregelen om de communicatie van ambtenaren met burgers, bedrijven en instellingen beter te beveiligen.
  De producten en -diensten die we hierbij gebruiken:
  - Digitale dienst 'Justitie Beveiligde Internet Toegang', kortweg JuBit
  - Voldoen aan de verplichte open standaarden
  - Blokkade van apps en websites uit landen met een offensief cyberprogramma

- IT continuïteit management
  Dit aspect richt zich op het opstellen en testen van herstelplannen voor de kritieke systemen. Een Computer Security Incident Response Team helpt een organisatie daarbij. Door positieve testen laten organisaties zien weerbaar te zijn na een groot incident of calamiteit.
  De producten en -diensten die we hierbij gebruiken:
  - CSIRT: Computer Security Incident Response Team
  - Herstelplannen en -testen

- Informatiebeveiligingsbeoordeling
  Dit laatste punt richt zich op de controle van de naleving van informatiebeveiligings-maatregelen. Via Governance Risk en Compliance wordt gewerkt aan een duurzame informatie-beveiligingsorganisatie waarbij de betrokken functionarissen risico-gebaseerd informatiebeveiligingsmaatregelen implementeren, evalueren en bijstellen waar nodig. De informatiebeveiligingsorganisatie maakt daarbij gebruik van goed gedocumenteerde risicomanagement- en incidentmanagementprocessen en -kaders, en wordt ondersteund door professionele GRC-tooling.
  De producten en -diensten die we hierbij gebruiken:
  - GRC-tooling: de digitale dienst 'Governance, Risk en Compliance' administratie
  - Red team onderzoeken
  - Technische beveiligingsonderzoeken naar kritieke systemen en compromittering

In 2024 worden de ondersteuning en monitoring van het gebruik van een centraal aantal resultaten overgedragen aan de lijnorganisatie. Hierdoor ontstaat ruimte voor nieuwe resultaten. Vooralsnog zijn zes onderwerpen aangewezen als resultaat-gebieden. Ze vloeien voort uit een analyse van de sterkten, zwakten, kansen en bedreigingen van de cyberweerbaarheid van het ministerie.

Drie onderwerpen zijn al in scope: gegevensclassificatie, leveranciersmanagement en toegangsbeveiliging voor gebruikers. Bij leveranciersmanagement gaat het om het op strategisch niveau managen van de relatie met de belangrijke leveranciers van de rijksoverheid - denk aan Microsoft, Google Cloud en Amazon Web Services. Onderdeel van die relatie is bijvoorbeeld door het neerzetten van en helder communiceren over juridische kaders, pro actief handelen bij nieuwe wetgeving en op ontwikkelingen bij deze leveranciers - zoals rondom AI, en adviseren over relevante vragen vanuit het Rijk in relatie tot de leverancier en andersom. Dit gebeurt vanuit een gespecialiseerd team.
De drie nieuwe onderwerpen zijn netwerksegmentatie, simulatie van aanvallen en inbreuken, en vertrouwensrelaties tussen technische domeinen. Momenteel worden de behoeften van de organisaties aan eventuele aanvullende onderwerpen geraadpleegd. Eind 2023 wordt besloten over de beoogde centrale resultaten voor 2024.

Inkoop en IV
Vanuit de afdeling 'Strategische Inkoop' worden IV-vragen en behoeften op verschillende manieren ondersteund. Dit varieert van eenvoudige inkooptransacties via de Inkoop Uitvoerings-centra, de IUC's, tot het uitvoeren van rijksbrede aanbestedingen van programmatuur. Het al eerder genoemde strategisch leveranciersmanagement (SLM) hoort ook bij deze gespecialiseerde afdeling. Voor SLM zijn rijksbrede overeen-komsten met Microsoft en Amazon Web Services afgesloten, met goede borging van belangrijke onderwerpen als bescherming van persoonsgegevens. Het SLM-team houdt de ontwikkelingen van nieuwe Europese wetgeving zoals de NIS2-richtlijn en AI-act nauwlettend in de gaten en legt de hieruit voortvloeiende noodzakelijke contractuele waarborgen met de strategische leveranciers vast. De juridische kaders zijn beschikbaar en toepasbaar voor alle rijksorganisaties.

Tenslotte
Naast het halen van de resultaten zelf, werkt de JenV-organisatie ook aan het beleid dat minimaal nodig is om de resultaten te halen. Dat geldt ook voor het in kaart brengen van de impact van nieuwe wet- en regelgeving - zoals de Wbni2 naar aanleiding van de NIS2-richtlijn. De implementatie van de NIS2-richtlijn bij JenV wordt mogelijk bij het programma IB2.0 belegd. Tenslotte geeft het jaarlijks herhalen van de SWOT-analyse[20] inzicht in mogelijke nieuwe onderwerpen.

Verbinding met de andere digitale thema's

Digitale agenda	(draagt bij aan) thema	
i-Strategie JenV 2022 - 2027	# 7	Digitale weerbaarheid
I-strategie Rijk 2021 - 2025	# 2	Digitale weerbaarheid
Werkagenda Waardengedreven Digitaliseren	§ 2.4.5	Overheden zijn overheidsbreed getraind om cyberincidenten te voorkomen

[20] De afkorting SWOT staat voor Strengths (sterktes), Weaknesses (zwaktes), Opportunities (kansen) en Threats (bedreigingen).

3.4 Nieuwe thema's i-Strategie

De vijf nieuwe thema's zijn, net als de eerder vastgestelde drie hiervoor genoemde thema's, met name ingegeven door de grote beleidsprioriteiten uit het tweede hoofdstuk.

3.4.1 Mensgerichte dienstverlening

Volgens de overheidsbrede visie op dienstverlening is voor het vormgeven van de publieke sector van de toekomst vergaande samenwerking tussen overheden nodig. Het doel is om de digitale overheid toegankelijker, begrijpelijker en persoonlijker te maken.
Bij een positieve gebruikerservaring horen eenvoudige processen. Zodat je aan de ene kant als burger weet wat je zelf moet doen en wat je van de overheid kunt verwachten. En zodat burgers zelf de regie hebben over hun eigen persoonsgegevens en ondersteund worden bij de uitoefening van hun rechten. Aan de andere kant gaat het ook over de medewerker die elke dag werkt aan die positieve ervaring en moet kunnen beschikken over de technologie die nodig is om de bijbehorende dienstverlening te kunnen bieden. Techniek die net zo goed beschikbaar is voor de doelgroep die van de dienst gebruik wil maken. Denk aan een justitiabele, het slachtoffer van een misdrijf of een kind in nood. Maar ook aan de politieagent op straat, de rechter op de zitting of de jeugdhulpverlener. Kortom: logische, samenhangende en toegankelijke dienstverlening.

Dit i-Strategiethema richt zich op 'de centrale plus': wat kan JenV centraal (generiek) organiseren of realiseren, waarmee we onze JenV-organisaties meerwaarde bieden bovenop hun eigen digitale dienstverlening. Een eenduidig antwoord op die vraag is best ingewikkeld en dat komt vooral door twee omstandigheden.

Als eerste de diversiteit in organisaties: er zijn grote verschillen in het niveau van digitale dienstverlening tussen de JenV-organisaties. Zo is een aantal onderdelen al flink op dreef met hun digitale dienstverlening, terwijl anderen nog aan het inventariseren zijn welk dienstverleningsconcept de meeste meerwaarde kan bieden. Daarnaast is er de diversiteit in klantgroepen. Bij de een heet de klant bijvoorbeeld bewoner, bij de ander gedetineerde, jeugdige, betrokkene, verdachte of slachtoffer. Bovendien neemt een gedetineerde of verdachte op een andere, niet geheel vrijwillige manier, JenV-diensten af dan bijvoorbeeld een bewoner van een asielzoekerscentrum of slachtoffer van een misdrijf. Ook hier zijn dus verschillende perspectieven die het onmogelijk maken er één ultiem dienstverleningsconcept op los te laten.

Om het eenduidige antwoord op de vraag - elementen van mensgerichte dienstverlening die overkoepelend kunnen bijdragen - te vinden, richt 'Mensgerichte dienstverlening' zich het eerst op de volgende aspecten:

1. Inzicht krijgen in de relevante ontwikkelingen in de omgeving van overheidsbrede dienstverlening en de toepassingsmogelijkheden voor JenV.
2. Inventarisatie van hoe nu digitale dienstverleningsconcepten in de praktijk werken en welke gedeelde uitdagingen er zijn te identificeren.
3. Verbinden op het gebied van digitale dienstverlening door te leren en inspireren - door kennisuitwisseling en het bieden van handvatten om goede voorbeelden toe te passen.

Beoogde resultaten

Het streven is eind 2023 voldoende overzicht te hebben van (gewenste) dienstverleningsconcepten, welke er al in de praktijk werken, en hoe deze ook voor anderen zouden kunnen werken. Op basis daarvan volgt in 2024 een aanpak om de IV in dienstverlening aan onze JenV-onderdelen meerwaarde te bieden. Dat kan bijvoorbeeld een kader zijn, een afsprakenstelsel, een set met architectuurprincipes, of een voorziening/ functionaliteit. En wellicht een combinatie.

Verbinding met de andere digitale thema's

Digitale agenda	(draagt bij aan) thema	
i-Strategie JenV 2022 - 2027	# 1	Mensgerichte dienstverlening
I-strategie Rijk 2021 - 2025	# 3	ICT-landschap: digitale toegang tot de dienstverlening is makkelijk en logisch
Werkagenda Waardengedreven Digitaliseren	geheel	De hele agenda is gericht op het verbeteren van digitale dienstverlening aan de samenleving

3.4.2 I in het hart van beleid, wetgeving en uitvoering

Bij I in het hart gaat het erom dat beleid, wetgeving en uitvoering samen de kansen van digitalisering pakken en dat I vanaf het begin in ontwerp, formulering en vervolgens in de toepassing van beleid en wetgeving wordt betrokken. De i-Strategie JenV is geen doel op zich maar een middel om de publieke waarde en effectiviteit daarvan te vergroten. De ambitie is (de doelen van) de i-Strategie te verbinden aan de doelen van beleids-, wetgevings- en uitvoeringsprocessen en vice versa.

Voor het thema I in het hart betekent dat:

1. (Beleids)medewerkers en (wetgevings)juristen weten op welke momenten ze in hun werkprocessen moeten nadenken over 'de I' in beleidsontwerpen en wetgevingstrajecten.
2. (Beleids)medewerkers en (wetgevings)juristen weten de weg naar adequate, inhoudelijke en procesmatige I-ondersteuning.
3. Hiervoor zijn I-professionals beschikbaar met een I-control-, expert- of adviesrol, die kennis hebben van het (beleids)domein waarin zij werken en snappen hoe de werkprocessen van beleids- en wetgevingscollega's er uit zien.

Beoogde resultaten
De afgelopen periode is uitgebreid gesproken met de CIO's van de beleids-DG's en een aantal CIO's van uitvoeringsorganisaties. Over hun wensen en verwachtingen waar het gaat om meer I in het hart. Dat leverde vier rode draden op die nu planmatig worden uitgewerkt:

- I steviger verankeren in het beleidsproces
  Om beleidsmedewerkers eerder en vaker na te laten denken over de I in beleid, moet I meer expliciet terugkomen in de handvatten om beleid te maken. We maken verbinding met het Beleidskompas.

- Versterken van de I-functie binnen beleidsdirecties
  Om beleidsmedewerkers echt te helpen met I-aspecten in het beleid dat zij maken, is het belangrijk deze hulp dicht tegen beleid aan te organiseren. De I-functie binnen de beleids-directies heeft daarvoor capaciteit, kennis en kunde nodig.

- Vergroten van de I-kennis van niet-I-professionals
  De beleidsdirecties willen graag hun I-kennis vergroten. Daarbij hebben verschillende doelgroepen verschillende behoeftes. Zo hebben eigenaren en opdrachtgevers van grote ICT-projecten behoefte aan handvatten om het opdrachtgeverschap te verbeteren, terwijl medewerkers die bezig zijn met digitalisering andere kenniswensen en -eisen hebben. In deze lijn wordt materiaal verzameld en ontwikkeld. Voor het aanbieden van het materiaal zoeken we de samenwerking met de JenV Academy en RADIO, de RijksAcademie voor Digitalisering en Informatisering Overheid.

- Verstevigen van de verbinding tussen beleid en uitvoering
  Juist voor de I is het belangrijk dat de uitvoering zo vroeg mogelijk betrokken wordt bij nieuw beleid, liefst nog voor een formele uitvoeringstoets. Niet alleen tussen het departement en de uitvoeringsorganisaties, maar ook tussen beleidsafdelingen en I-afdelingen in de uitvoeringsorganisaties. Het gaat er om de juiste organisatieonderdelen met elkaar te verbinden.
  Een instrument als een beleidskalender kan hierbij onder-steuning bieden.

Verbinding met de andere digitale thema's

Digitale agenda	(draagt bij aan) thema	
i-Strategie JenV 2022 - 2027	# 2	I in het hart van beleid, wetgeving en uitvoering
I-strategie Rijk 2021 - 2025	# 1	I in het hart
Werkagenda Waardengedreven Digitaliseren	§ 4.3.2	De opbouw van een professionele IT/IV-organisatie (...in het hart van beleid, uitvoering, toezicht en handhaving...)

3.4.3 Versterking van de besturing van de informatievoorziening

Op het gebied van informatievoorziening (IV) worden steeds meer en hogere eisen gesteld, inclusief waarborgen waarvoor de bestuurder moet instaan. IV-zaken hebben impact op vrijwel alle activiteiten en ambities van ons ministerie en haar organisaties. Dit vraagt om een herijking van de bestaande governancestructuur om de besturing van de IV te versterken. Daar horen ook mechanismen bij om tijdig te acteren op nieuwe eisen en wensen van de JenV-organisaties, en de eisen en wensen die van buitenaf komen - zoals van andere ministeries, de Tweede Kamer en Europa. Investeren in besturing, digitaal leiderschap en governance is noodzakelijk om de volgende stappen in de digitale transformatie te kunnen zetten. De I wordt volwassener, en daar hoort een volgend niveau van besturing van de IV bij.

Beoogde resultaten
Door de verschillende rapportageprocessen beter te laten aansluiten op de begrotingscyclus, kunnen we de informatie en investeringen die nodig zijn voor een betere informatievoor-ziening slimmer en efficiënter gebruiken. Dat is de kern van het thema Versterking besturing. De uitwerking gebeurt langs drie lijnen, met selectie uit de beoogde resultaten:

- Planning en verantwoording IV
  Doel: overzicht en inzicht in de status van het JenV IV-landschap
  Op dit punt wordt concreet gewerkt aan meerjarige informatie-plannen. Nog niet alle JenV-organisaties beschikken over een meerjaren informatie(beleids)plan dat inzicht en overzicht geeft over de eigen informatieplanning en -voorzieningen. Een meerjarige informatieplanning (inclusief financiële paragraaf) is ook nodig om op tijd aan te kunnen sluiten bij de financiële processen - bijvoorbeeld wanneer de noodzaak ontstaat voor aanvullende financiering. Ook staan vanaf 2024 onder andere een jaarlijkse actualisatie van het (meerjarig) departementaal informatieplan en een geïntegreerde managementrapportage vanuit het perspectief van de CIO en hoofddirecteur Bedrijfsvoering op de rol.

- Financiën IV
  Doel: stabiele (toekomstvaste) financiering van het JenV IV-landschap
  Toekomstvaste financiering van de JenV-informatievoorziening is een belangrijk aspect van een sterke besturing. De digitale transformatie vraagt om meerjarig plannen en daar horen meerjarige budgetten en financieringsafspraken bij, passend binnen de begrotings-cyclus. De verdere stroomlijning van het gezamenlijke begrotingsproces voor de JenV-informatie-voorziening is voorzien vanaf de Voorjaarsnota 2024. Vanaf 2025 is het streven het IV-planning en -controlproces volledig aan te laten sluiten op het begrotingsproces.

- Besturing IV
  Doel: inzicht in en terugdringen van de rapportagelast
  In 2020 is een evaluatie uitgevoerd naar de werking- en gewenste verbeteringen van het CIO-stelsel JenV. Ook is met het Besluit CIO-stelsel Rijksdienst 2021 het kader voor de organisatie-inrichting van het CIO-stelsel aangescherpt. Op dit moment wordt de uitbreiding van het CIO-stelstel met een Chief Data Officer (CDO-), Chief Technology Officer (CTO-) en Chief Privacy Officer (CPO-) functie voorbereid. In 2024 wordt daarnaast gewerkt aan een gestandaardiseerd sturingsmodel voor digitale diensten, projecten/programma's en verandertrajecten, en een JenV-brede kalender voor digitaliseringstrajecten. En door onder andere rode draden uit CIO-oordelen te halen en meer integraal te kijken naar (de opvolging van) adviezen uit BIT-toetsen, zorgen we voor betere uitvoering van onze grote ICT-activiteiten. Voor de langere termijn onderzoeken we de intensivering van de samenwerking met andere dienstverleners in het JenV-domein, zoals deurwaarders en advocaten.

Verbinding met de andere digitale thema's

Digitale agenda	(draagt bij aan) thema	
i-Strategie JenV 2022 - 2027	# 3	Versterking van de besturing van de IV
I-strategie Rijk 2021 - 2025	# 9	I-besturing
Werkagenda Waardengedreven Digitaliseren	§ 4.3.2	De opbouw van een professionele IT/IV-organisatie (...effectieve besturing...)

3.4.4 Doorontwikkeling digitaal grondvlak

Het zogenaamde 'Digitaal grondvlak' is het snijvlak waarop de interactie tussen afnemers en aanbieders van IV-voorzieningen plaatsvindt. Het is de plek waar de gemeenschappelijke IV-voorzieningen die door meerdere JenV-organisaties worden gebruikt, worden gecreëerd en onderhouden. Met een combinatie van besturingsprocessen, dienstverlening en techniek biedt het digitaal grondvlak een gemeenschappelijke basis met voorzieningen en (gegevens) diensten naar JenV-onderdelen, andere overheidsorganisaties, burgers en bedrijven.

JenV heeft al veel bereikt op dit gemeenschappelijk grondvlak, waarbij de afgelopen jaren de nadruk lag op uitbreiding van het aantal IV-voorzieningen. De komende jaren spelen we in op een toename van afnemers binnen en buiten JenV, toenemende cyberdreigingen, steeds snellere technologische ontwikkelingen, complexere bewerkingen van (persoons)gegevens, snellere implementaties van wet- en regelgeving en hogere milieueisen. Dat betekent dat onze IV-voorzieningen beheersbaarder, toegankelijker, duurzamer en flexibeler moeten worden.
Het i-Strategiethema Doorontwikkeling digitaal grondvlak draagt hier aan bij.

Daarvoor zijn de volgende doelen gesteld:

1. Optimalisatie gebruik van het Digitaal grondvlak
   Gemeenschappelijk beeld van de (huidige) behoeftes van afnemers en (huidige) diensten van aanbieders om inzicht te krijgen in de elementen die samen onderdeel uit gaan maken van het Digitaal grondvlak.
2. Diensten en voorzieningen beschikbaar via een gedeelde catalogus
   Heldere, overzichtelijk en inzichtelijke catalogus van de diensten en voorzieningen van het Digitaal grondvlak.
3. Eenduidige besturing van diensten en voorzieningen
   Vanuit een gezamenlijke visie en ambitie besturen van diensten en voorzieningen zodat deze passen bij de situatie van de afnemer.
4. Gegevens eenduidig en duidelijk ter beschikking stellen
   Met behulp van het Digitaal grondvlak mogelijk maken om gevoelige (persoons)gegevens te ontdoen van tot de persoon herleidbare kenmerken en te zorgen voor een integrale toegangsvoorziening en proactieve monitoring voor rechtmatig gebruik.
5. Diensten en voorzieningen eenduidig beschikbaar stellen
   Continu monitoren van de 'gezondheid' en op- en afschalen van de diensten en voorzieningen naar gelang van de wens van de afnemer.

In 2023 wordt het streefbeeld vastgesteld (het 'wat') van het Digitaal grondvlak, met daarbij de aanpak (het 'hoe' en 'wanneer'). Ook starten we met de eerste contouren van de catalogus, om in 2024 een eerste versie te realiseren.

Verbinding met de andere digitale thema's

Digitale agenda	(draagt bij aan) thema	
i-Strategie JenV 2022 - 2027	# 4	Doorontwikkelen digitaal grondvlak
I-strategie Rijk 2021 - 2025	# 4	Generieke voorzieningen
Werkagenda Waardengedreven Digitaliseren	§ 4.3.1	Verbeterde IT/IV-systemen en infrastructuur
	§ 4.3.2	De opbouw van een professionele IT/IV-organisatie (...en de daarvoor vereiste IT/IV-systemen ontwikkelen...)

3.4.5 Beheerste vernieuwing

Het beheersen van het IT-landschap en het vernieuwen ervan is een randvoorwaarde voor veel van de doelstellingen van onze i-Strategie. Achterstallig onderhoud leidt tot risico's, die duidelijk worden bij ontbrekende of onvoldoende support, en op hun beurt leiden tot ad-hoc acties onder tijdsdruk. De verhoogde risico's zijn divers; denk aan een kwetsbare informatiebeveiliging, datalekken, verstoringen in de continuïteit van de dienstverlening en steeds minder ruimte voor noodzakelijke vernieuwing.
In het Besluit CIO-stelsel Rijksdienst 2021 is opgenomen dat de departementale CIO verantwoordelijk is voor (de kaderstelling op) het ontwikkelen en coördineren van integraal portfoliomanagement en (de kaders voor) het bijbehorende levenscyclusmanagement van ICT-systemen. Lifecycle management, kortweg LCM, gaat over 'weten wat je in huis hebt' qua applicaties en systemen en de status daarvan.
JenV-breed is al goed zicht op wat in huis is. We leren van elkaar en worden steeds beter in het nemen van volgende stappen in volwassenheid. Veel van de JenV-onderdelen hebben al een aanpak liggen voor het wegwerken van hun technische schuld.

Dit nieuwe i-Strategiethema heeft tot doel aspecten van 'beheerste vernieuwing' een stabiel onderdeel te maken van bestaande en nieuwe processen en planvorming binnen de JenV-organisaties. Door georganiseerd samen te werken, en bestaande processen en hulpmiddelen te optimaliseren kunnen we huidige risico's beter beheersen, nieuwe technische schuld zoveel mogelijk voorkomen en meer ruimte creëren voor vernieuwing.

Beoogde resultaten
Onder de vlag van Beheerste vernieuwing bieden we overkoepelende vraaggestuurde hulpmiddelen en herijken we waar nodig bestaande processen en kaders. Ook ontwikkelen we de JenV-brede nulmeting van het volwassenheidsniveau door tot een gevalideerde 1-meting.

Maar daarmee zijn we er nog niet. Het serieus werk maken van daaropvolgende technische stappen - zoals het wegwerken van legacy, het plegen van onderhoud, en het plannen en begroten van (door)ontwikkeling - moet ervoor zorgen dat ons IV-landschap ook echt op orde blijft. Daarvoor komt onder meer een JenV-brede legacy-roadmap - als product van steeds beter inzicht in het applicatielandschap - en een duidelijke vernieuwingsvisie op hoe we ruimte creëren voor een toekomstvaste informatievoorziening. Naast de techniek zal ook een volgende stap gezet moeten worden bij de inrichting van huidige (werk)processen en het faciliteren van onze medewerkers om hun LCM-volwassenheidsniveau in denken en doen te verhogen.

Verbinding met de andere digitale thema's

Digitale agenda	(draagt bij aan) thema	
i-Strategie JenV 2022 - 2027	# 8	Beheerste vernieuwing
I-strategie Rijk 2021 - 2025	# 3 # 8	ICT-landschap Transparantie en inzicht
Werkagenda Waardengedreven Digitaliseren	§ 4.3.1	De opbouw van een professionele IT/IV-organisatie (...effectieve besturing...)
	§ 4.3.3	Transparante en inzichtelijke kosten, baten, samenhang en status van ICT-activiteiten

Hoofdstuk 4

Risico's en Randvoorwaarden

De i-Strategie JenV geeft, samen met de informatieplannen, de strategische veranderkoers en de ontwikkelrichting weer voor de I(CT)-voorzieningen. De drie eerder in gang gezette thema's Digitale weerbaarheid, Informatiehuishouding en Gegevens en algoritmes lopen al. Voor de andere vijf geldt dat zij deels nog in de opstartfase zijn. Dat vergt investeren in personele capaciteit en financiële middelen.

De grootste risico's die op dit moment spelen, gelden zeker niet alleen voor de i-Strategie, maar zijn JenV-breed van toepassing op onze hele IV-opgave. Voor de eerste paragraaf, de uitvoerbaarheid van de opgenomen beleidsprioriteiten, is het zelfs een harde disclaimer.

4.1 Uitvoerbaarheid

De in dit informatieplan opgenomen beleidsprioriteiten zijn ambities, waarvoor in sommige gevallen de detailuitwerking nog niet klaar is en de middelen nog niet volledig zijn toegekend.
De verwachtingen in de mate waarin IV kan bijdragen aan het realiseren van de beleidsambities zijn hoog. Tegelijkertijd zijn onze inspanningen doorlopend gericht op het digitaal weerbaar blijven. De inzet op digitale weerbaarheid - en bijbehorende forse capaciteit die daarvoor nodig is - blijft een belangrijke randvoorwaarde voor het succesvol uitvoeren van onze opgaven. Opgeteld veroorzaakt dit voor onderlinge concurrentie op de absorptiecapaciteit van de JenV-organisaties, en noopt daarmee tot het maken van keuzes in de uitvoerbaarheid. Zowel beleidsmatig als financieel.
Om aan te blijven sluiten op de behoeften vanuit de samenleving, wordt op gezette momenten in de beleids- en begrotingscyclus gekeken of de prioriteiten nog steeds voldoende in de portfolio, absorptievermogen en financiële kaders van de JenV-organisaties passen.

De indruk wekken dat het IV-domein alleen draait om de in dit informatieplan genoemde beleidsprioriteiten met een IV-component, zou een verkeerd beeld geven. Het grootste deel van het werk zit namelijk in de reguliere bezigheden: het beheer en onderhoud - inclusief de doorontwikkeling - van het IV-landschap. Ook hierbij worden binnen het budgettair kader afwegingen gemaakt tussen beheer en onderhoud aan de ene kant, en vernieuwing aan de andere kant. Met oog voor wat een organisatie aankan qua verandering.

4.2 Absorptievermogen

Er komt (te) veel op ons af. Denk aan maatschappelijke en politieke verwachtingen, technische mogelijkheden en de bijbehorende veranderopgaven. En dat terwijl de JenV-organisaties al veel op zich af zien komen. Vanuit veranderingen in wet- en regelgeving, beleidsveranderingen en wensen vanuit de organisaties zelf wordt er al een groot beroep gedaan op het absorptievermogen van de verschillende JenV-organisaties.
Ons absorptievermogen wordt ver overvraagd en dus zullen we moeten prioriteren. Dat prioriteren kan ertoe leiden dat in dit informatieplan genoemde opgaven bijvoorbeeld in de tijd gefaseerd(er) worden ingevoerd. De CIO-raad prioriteert onder andere met behulp van de 'Implementatiekalender Digitalisering'[21]: een JenV-brede implementatiekalender voor de digitaliserings-opgaven van de komende jaren.

[21] De Implementatiekalender Digitalisering, de IKD, is een intern document en op aanvraag beschikbaar.

4.3 Kennis en capaciteit

De arbeidsmarkt is zo overspannen dat beschikbare capaciteit - zowel kwantitatief als kwalitatief - steeds vaker een beperkende factor zal zijn voor het realiseren van de gestelde doelen. Met name vakprofessionals op cyberweerbaarheid zijn bijzonder schaars.

Daarnaast heeft ook JenV te maken met uitstroom van medewerkers en blijven we zoeken naar nieuwe - soms nationaal nog niet eens beschikbare - kennis voor innovatie.
Dat maakt ook de uitvoering van de i-Strategie tot een vraagstuk voor P&O en management.

JenV richt zich proactief en intensief op het boeien én binden van talent op i-gebied. Met professionele werving en ontwikkelpaden ontwikkelen we een werkomgeving waarin i-professionals graag komen én zich blijven ontwikkelen. JenV maakt daarbij gebruik van een aantal initiatieven uit het rijksbrede I-strategiethema I-vakmanschap. Bijvoorbeeld de samenwerking met het hoger onderwijs via I-Partnerschap en de inzet van Rijks I-trainees.
In huis is er de JenV Academie, rijksbreed is er RADIO, en ondertussen trekken we samen op met de directie Personeel en Organisatie voor strategische i-Personeelsplanning.
En dan nog kan het gebeuren dat vanwege schaarste alsnog moet worden geprioriteerd.

4.4 Stabiele financiering

Een goede informatievoorziening ondersteunt een efficiënte en effectieve invulling van onze beleidsprioriteiten. Anders gezegd: de keuze voor investeren in IV, is ook kiezen voor een betere uitvoering van beleid. Daarbij komt dat we een euro maar één keer kunnen uitgeven, en IV één van de onderwerpen is op het totaal van bestuurlijke besluitvorming over prioriteiten. Door de sturing op de IV beter te laten aansluiten op de begrotingscyclus, wordt het maken van bestuurlijke afwegingen in de besteding van beschikbare middelen gebalanceerder.

Met de vele ambities op digitalisering is zogenaamde 'stabiele financiering' een randvoorwaarde geworden voor een efficiënte uitvoering van dit meerjarig informatieplan.
Stabiele financiering gaat over het slim en vooraf gepland inzetten van middelen voor toekomstvaste IV. om te voorkomen dat er na verloop van tijd structurele problemen ontstaan voor de vervanging. We onderzoeken de komende periode op welke manier dit voor JenV zou kunnen werken.

4.5 Prioritering en/in het CIO-stelsel

Verschillende dienstonderdelen willen verder intensiveren op de uitwerking en de implementatie van de i-Strategie. Bijvoorbeeld door te investeren in de Chief Data Officer (CDO-), Chief Technology Officer (CTO-) en Chief Privacy Officer (CPO-) taken die voortvloeien uit de eind dit jaar verwachte uitbreidingen van het CIO-stelsel - de Chief Information Officer (CIO) en Chief Information Security Officer (CISO) zijn al bestaande rollen in het huidige Besluit CIO-stelsel. Niet alle ambities kunnen op dit moment, prioritering is dus noodzakelijk.

Planning en verantwoording
Via de 'Staat van IV' houdt de CIO van JenV de voortgang van de uitvoering van de i-Strategie in de gaten. De Staat van IV wordt komend jaar door ontwikkeld tot een 'IV in Beeld' om de CIO JenV beter in positie te brengen om te sturen op IV.
IV in Beeld omvat de informatie over de knelpunten, risico's, en meer algemene stand van zaken van de uitvoering van het departementale ICT-beleid. Vanuit de sturingsverantwoordelijkheid is IV in beeld te verdelen in twee categorieën:

- 'Continuïteit van IV' met informatie over de staande en toekomstige IV/ICT (beheer en vernieuwing) zoals dat bij de JenV-onderdelen is ingericht en waarover de eigenaar wordt geadviseerd.
- 'i-Strategie' met informatie over de bijdragen van de JenV-onderdelen aan de i-Strategie waarbij met minimaal één kpi per i-Strategiethema wordt gestuurd op de voortgang.

Oordelen, toetsen en audits
Voor grote ICT-activiteiten voert JenV CIO-oordelen uit, zoals in het Besluit CIO-stelsel Rijksdienst staat. Er worden ook andere audits uitgevoerd, om indien nodig bij te sturen.

Het Adviescollege ICT-toetsing (AcICT) toetst zelfstandig de projecten binnen de centrale overheid. Dit zijn de zogenaamde BIT-toetsen waarbij gekeken wordt naar de beheersbaarheid van projecten en programma's met een meerjarige ICT-component van meer dan € 5 miljoen. De bewindslieden van JenV sturen deze adviezen met een reactie naar de Tweede Kamer. Op het Rijks ICT-dashboard staat meer informatie over de projecten van JenV met een ICT-component van tenminste € 5 miljoen, over de hele looptijd van het project.

De Auditdienst Rijk doet als interne auditer gevraagd en ongevraagd onderzoek. Dat gebeurt op basis van haar wettelijke taak met accountantscontrole en met onderzoek naar gevoerd begrotingsbeheer, financieel beheer en de materiële Bedrijfsvoering. Daarnaast onderzoekt de Auditdienst de uitvoering van en beleids- en bedrijfsvoering, en grote ICT-projecten.

De Algemene Rekenkamer tenslotte controleert de inkomsten en uitgaven van de rijksoverheid en rapporteert hierover aan de Tweede Kamer in het jaarlijkse Verantwoordingsonderzoek. Deze externe toezichthouder doet ook onderzoek naar de kosten en effecten van overheidsbeleid.

4.6 Begroting

De benodigde budgetten voor de beleidsprioriteiten en IV-activiteiten en -producten zijn zoveel als mogelijk gedekt vanuit de reguliere middelen. Daar waar nog geen middelen beschikbaar zijn, wordt geprioriteerd, worden resultaten gefaseerd, dan wel wordt in de reguliere begrotingscyclus alsnog dekking gevraagd. Met name voor de Europese wetgevingsagenda geldt dat dekking nog een aandachtspunt is; dat betekent prioritering in de portfolio's van de individuele JenV-organisaties.

Er zijn er drie soorten digitaliseringsactiviteiten te onderscheiden:

Beleidsinitiatieven die bijdragen aan grotere digitaliseringsbewegingen
Hierbij gaat het om digitaliseringsactiviteiten die voortkomen uit de beleidsprioriteiten, maar die (nog) niet strikt af te bakenen zijn in ICT-activiteiten.

Beleidsinitiatieven die leiden tot afgebakende ICT-activiteiten
Hierbij valt te denken aan vernieuwings- en vervangingsprojecten. Deze ICT-activiteiten zijn, samen met hun planning en begroting, terug te vinden op het Rijks ICT-dashboard[22].

JenV-overkoepelende IV-activiteiten en -producten
Deze digitaliseringsactiviteiten worden uitgevoerd onder de vlag van de i-Strategie JenV 2022 - 2027. Daarbij hebben de drie thema's die al langer lopen - Digitale weerbaarheid, Gegevens en algoritmes en Informatiehuishouding - hun eigen financieringslijn. Het programma Open op Orde wordt grotendeels gefinancierd vanuit gelden die het ministerie van Binnenlandse Zaken en Koninkrijksrelaties beschikbaar stelt.
De dekking voor planvorming voor de vijf nieuwe thema's - Mensgerichte dienstverlening, I in het hart, Versterking besturing, Digitaal grondvlak en Beheerste vernieuwing - komt in eerste instantie vanuit de gereserveerde gelden voor de uitvoering van de i-Strategie JenV. De aanvraag voor middelen die per thema extra nodig zijn, lopen mee in de reguliere begrotingscyclus.

[22] De ICT-activiteiten van JenV op het Rijks ICT-dashboard.

Dit informatieplan is een uitgave van

Ministerie van Justitie en Veiligheid
Directie Informatievoorziening & Inkoop

Meer informatie | i-strategie@minjenv.nl

November 2023