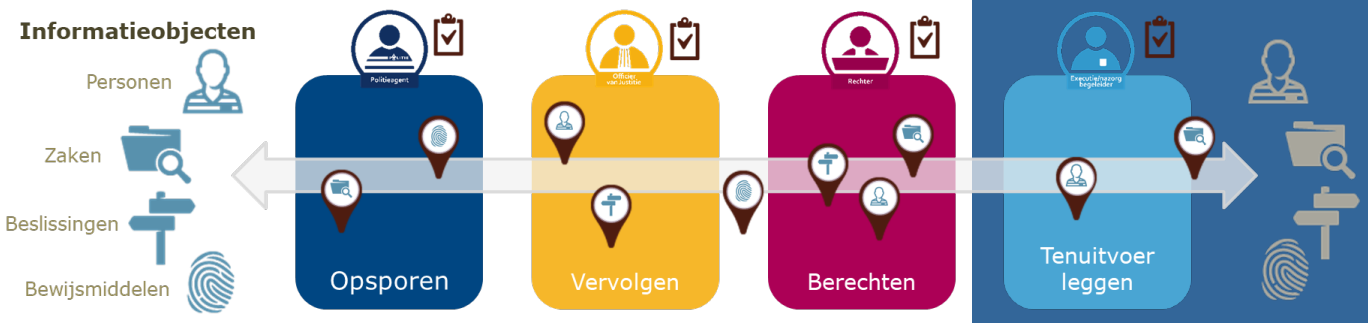
Strafrechtketen Architectuurraad

Verdieping Ketendoelarchitectuur Strafrechtketen

oktober 2021



Mantra: SRK-AR
De strafrechtketen kan digitaal, betrouwbaar, veilig en eenvoudig gegevens over personen, 'zaken', beslissingen en bewijsmiddelen uitwisselen. Zo zijn deze gegevens vanuit ieder gewenst perspectief, binnen en buiten de keten tijdig en volledig beschikbaar, voor iedereen die ze nodig heeft en mag gebruiken, om te kunnen handelen, beslissen, leren, besturen en verantwoorden.

Colofon

Opdrachtgever	Opdrachtgevers Beraad (OGB)
Titel	Verdieping Ketendoelarchitectuur Strafrechtketen
Auteur Programma	Strafrechtketen Architectuurraad (SRK-AR)
Datum	29 oktober 2021
Versie	1.0
Status	Vastgesteld door OGB 28 oktober 2021
Mail	ArchitectenSRK@minjenv.nl
Online	https://www.astraonline.nl

Inhoudsopgave

Status document

Dit document is opgesteld door de SRK-AR (Strafrechtketen Architectuurraad) in opdracht van het Opdrachtgeversberaad (OGB). De leden van de SRK-AR komen vanuit de ketenpartners, op het moment van schrijven zijn dat de Politie, het Openbaar Ministerie, de Rechtspraak (rechtbanken en hoven), Reclassering Nederland, de Koninklijke Marechaussee, Justitiële Informatiedienst, Dienst Justitiële Inrichtingen, Centraal Justitieel Incassobureau, Jeugdzorg, Raad voor de Kinderbescherming, en de keten-ondersteunende afdelingen KIV, Ketenregie en Directie Strafrechtketen ondergebracht bij het ministerie van JenV. De leden van de SRK-AR handelen daarbij vanuit hun kennis en expertise en vervullen een liaison rol naar hun achterban.

Bij vaststellen van de Ketendoelarchitectuur 1.0 (KDA), september 2020 door het OGB, is aangegeven dat de KDA een levend document is. Onderdelen, zoals ketencommunicatievoorzieningen en transitie, waren nog open of vroegen om een nadere uitwerking.

De SRK-AR kreeg bij het uitdragen en bespreken van de KDA met projecten en opdrachtgevers vragen om verduidelijking en verdieping. Thema's als rechtsstatelijkheid en digitale soevereiniteit verdienen een extra duiding.

Voorliggend document is daar de invulling van en is verder vooral een aanvulling, verduidelijking en verdieping van de KDA. Er zijn nuanceringen t.o.v. de KDA 1.0, geen herzieningen. Daar waar tegenstrijdigheden lijken te ontstaan met KDA 1.0 is de Verdieping KDA leidend.

In de KDA 1.0 zijn ook de diensten en werkwijze van de SRK-AR aangekondigd. Deze zullen 2e helft 2021 worden aangeboden voor vaststelling. Daarmee zijn de bij KDA 1.0 gedane toezeggingen nagekomen.

Wijzigingen t.o.v. de KDA 1.0

Om misverstanden te beperken zijn tekstuele en begripswijzigingen doorgevoerd. Zo is het mantra eenduidiger geformuleerd om verwarring over gegevens over personen met de concrete personen te voorkomen.

Het woord "notificatie" wordt veelal geassocieerd met berichtenverkeer op de technische laag, in plaats van het interactiepatroon "Notificatie". Dat zorgt in de praktijk regelmatig voor spraakverwarring. Daarom is dat interactiepatroon hernoemd naar "Attendering". Notificatie is daarmee beperkt tot de technische laag.

Het interactiepatroon "Attendering" heeft ook de vertaling gekregen naar de ketencommunicatievoorziening E-Makelaar. Waarmee het de aandacht heeft gekregen die in KDA 1.0 ontbrak.

Om verwarring met forensisch onderzoek te vermijden is het begrippenpaar chain-of-custody en chain-of-evidence vervangen door respectievelijk bewaarketen en bewerkingsketen.

Dankwoord

De SRK-AR dankt iedereen, in het bijzonder het project Ketenvoorzieningen en de vele reviewers, voor de kritische commentaren en de bijdragen aan dit document.

Correctie

Voorbeeld over VIP, blz. 52, gecorrigeerd. (okt. 2021)

Leeswijzer

De Ketendoelarchitectuur (KDA) en de Verdieping richt zich hoofdzakelijk op het "leidingwerk" dat informatie-uitwisseling tussen ketenpartijen in en van de strafrechtketen mogelijk maakt, en beschrijft daarom vooral de uitgangspunten en kaders voor interoperabiliteit op semantisch en technisch niveau. De totale strafrechtketenarchitectuur is groter en omvat, naast de KDA, o.a. een businessarchitectuur met beschrijvingen van en afspraken over verantwoordelijkheden, diensten, processen in en met de keten. In hoofdstuk 1 "Positioneren Strafrechtketenarchitectuur en de Ketendoelarchitectuur" wordt de scope van de KDA en de Verdieping nader toegelicht.

Dit betekent dat de Verdieping vanuit bedrijfsperspectief gezien abstract en "technisch" is.

Doelgroepen

De Verdieping bedient uiteenlopende doelgroepen.

De leden van het Opdrachtgevers Beraad (OGB) en het Coördinerend Beraad Executie (CBE) vormen de eerste doelgroep. Zij stellen de Verdieping vast. Voor deze doelgroep is met name hoofdstuk 2 "Kerngedachten Ketendoelarchitectuur" geschreven omdat daarin de uitgangspunten worden benoemd die de bestuurlijke richting geven aan de uitwerking van de KDA. De andere, voor bestuurders relevante hoofstukken, 6 "Ketencommunicatievoorzieningen conceptueel" en 8 "Transitiestrategie", zijn eerder door het OGB vastgesteld.

De I-adviseurs van de bestuurders en de I-adviseurs op strategisch en tactisch niveau vormen de tweede doelgroep. Afhankelijk van wijze van organiseren vaak onderdeel van een CIO-Office. Met het doorgronden van de KDA zienswijze op interoperabiliteit en transitiestrategie kunnen zij hun bestuurders en opdrachtgevers gericht adviseren over prioriteiten en samenstelling van het projectenportfolio.

Architecten, informatiemanagers, analisten en portfoliomanagers, programma- en projectleiders vormen de derde doelgroep. Het geeft hen handvatten voor de inrichting van de eigen IV en de inzet van communicatievoorzieningen die nodig zijn om interoperabiliteit in de realisatie te waarborgen. Het geeft een begrip en kaders om tot nadere afspraken in de strafrechtketen te komen.

Verder staat het uiteraard iedereen vrij om kennis te nemen van de KDA en de Verdieping. Zoals gezegd, de KDA gaat over interoperabiliteit en het onderliggend "leidingwerk" in de keten. Voor medewerkers uit het primair proces, politieagent, OvJ, Rechter, PIW'er, etc. is dat ver van hun bed. En dat moet het ook zoveel mogelijk blijven. Voor hen moet het "gewoon" werken.

Opbouw van het document

Hoofdstuk 1 "Positioneren Strafrechtketenarchitectuur en de Ketendoelarchitectuur" plaatst de KDA in de totale strafrechtketenarchitectuur. Dit hoofdstuk is bedoeld voor architecten en informatiekundigen.

Hoofdstuk 2 "Kerngedachten Ketendoelarchitectuur" beschrijft de essentie van de Ketendoelarchitectuur. Voor alle lezers relevant om kennis van te nemen.

Hoofdstuk 3 "Rechtsstatelijkheid en digitale datasoevereiniteit" en hoofdstuk 4 "Keteninformatisering" verdiepen de essentiële begrippen van de ketenarchitectuur. In hoofdstuk 3 worden ook veel gebruikte oneliners kritisch tegen het licht gehouden. In hoofdstuk 4 gaan we in op keteninformatisering en welke afspraken voor de strafrechtketen zijn gemaakt. Deze twee hoofstukken zijn voor alle lezers, m.u.v. bestuurders, het noodzakelijke startpunt voor verdere verdieping.

In hoofdstuk 5 Informatiemodel gaat over een stelsel van begrippen om onderscheid te kunnen maken tussen origineel, kopie, verschijningsvorm etc. Dit hoofdstuk is meer conceptueel en theoretisch. Het is bedoeld voor architecten en informatiekundigen.

Hoofdstuk 6 Ketencommunicatievoorzieningen conceptueel bezien en hoofdstuk 8 Transitiestrategie zijn eerder als afzonderlijke notities in het OGB behandeld. De teksten zijn, op correctie van taalfouten na, ongewijzigd. In de teksten van "Kerngedachten Ketendoelarchitectuur" en "IV organiseren in de keten" is op onderdelen verdere concretisering aangebracht. De hoofdstukken zijn relevant voor alle doelgroepen.

Hoofdstuk 7 Ketencommunicatievoorzieningen uitwerking gaat dieper in op de ketencommunicatievoorzieningen (afspraken, standaarden en ICT-functionaliteit). Het resultaat van eerdere informele documenten en gesprekken in de SRK-AR en met het programma Ketenvoorzieningen. Dit hoofdstuk is bedoeld voor architecten, projectleiders en analisten.

Vanaf hoofdstuk 3 wordt ieder hoofdstuk met een pagina cursieve tekst ingeleid.

Omdat de hoofdstukken van de Verdieping verschillende doelgroepen bedienen en het uitgangspunt is dat ieder hoofdstuk zelfdragend is, is het onvermijdelijk dat er soms herhalingen zijn. Die zullen vooral de lezer opvallen die alle tekst tot zich neemt.

Terminologie: Ketenpartner en ketenpartij

We maken in de KDA onderscheid tussen ketenpartner en ketenpartij.

Een ketenpartner is een organisatie(onderdeel) welke binnen de strafrechtketen opereert en daarmee een verantwoordelijkheid heeft in het traject van "incident tot en met interventie". Zoals daar o.a. zijn: Politie, KMar, Bijzondere Opsporingsdiensten, Openbaar Ministerie, Rechtspraak, Hoge Raad, CJIB, DJI, 3RO, NFI, Raad voor de Kinderbescherming, Jeugdzorg Nederland. Voor de volledige lijst zie https://www.strafrechtketen.nl/partners.

Een ketenpartij is een ketenpartner of een organisatie(onderdeel) die diensten levert aan of afneemt van de strafrechtketen. Dit breidt de kring uit met organisaties als de Belastingdienst, zorginstellingen, Veilig Thuis, UWV, SVB, etc.

Technische aanwijzingen

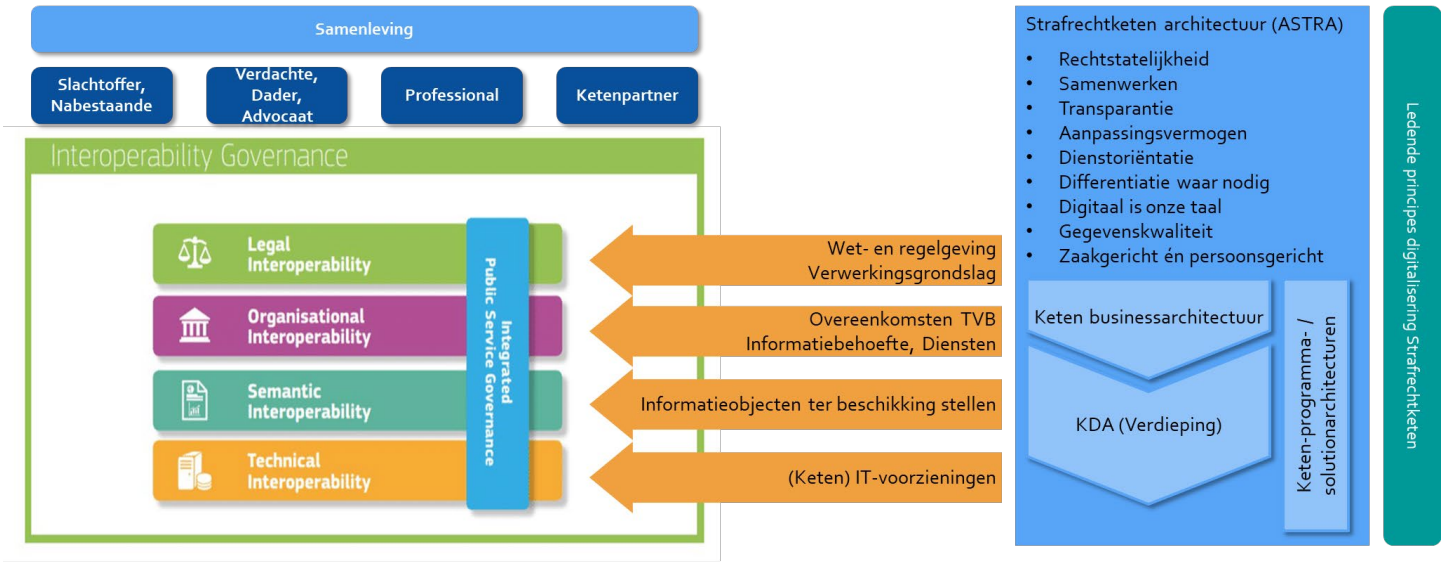
Schrijfwijze: rechtsstatelijk met dubbel 's'.
Schrijfwijze: rechtsstaat met dubbel 's'
Schrijfwijze: strafrechtketen zonder tussen 's'
Schrijfwijze: ketencommunicatievoorzieningen beginnen met twee hoofdletters. Dus E-Makelaar.
Schrijfwijze: Meervoud afkorting Ketencommunicatievoorzieningen: KCV'en.

Verwijzingen: Naar bronnen wordt verwezen door blokhaken en drie tot vier letters. [ABCD]. In "Bijlage 2: Referenties en afkortingen" zijn de verwijzingen opgenomen.

In de tekst worden drie symbolen gebruikt:

☞	Aanwijzing of dringende aanbeveling
!	Overweging, good practice
?	Nog uit te zoeken, uit te werken

Positioneren Strafrechtketenarchitectuur en de Ketendoelarchitectuur



Figuur 2 Strafrechtketenarchitectuur, businessarchitectuur en ketendoelarchitectuur en de relatie met het EIF-Raamwerk

1.1 De Strafrechtketenarchitectuur

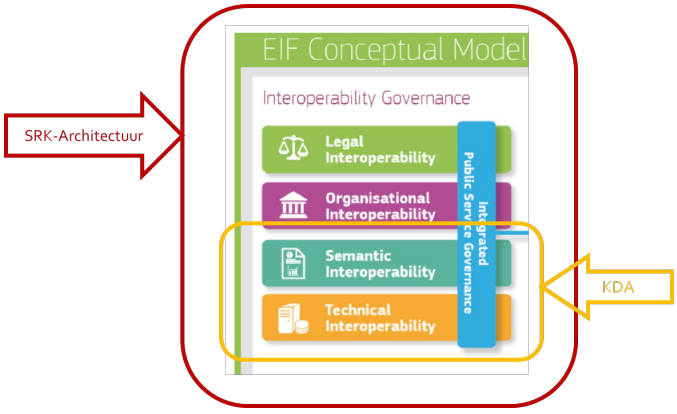
De strafrechtketenarchitectuur omvat alle afspraken en voorzieningen die in de strafrechtketen nodig zijn om als (soevereine) organisaties te kunnen samenwerken gericht op het bereiken van gezamenlijke doelen. Dat vermogen om te kunnen samenwerken noemen we interoperabiliteit.

Om hierover met elkaar te kunnen redeneren gebruiken we het EIF-Raamwerk[1] voor interoperabiliteit voor overheden. Het raamwerk maakt duidelijk dat de afspraken zich uitstrekken van juridische interoperabiliteit tot de technische interoperabiliteit. En dat deze lagen in samenhang gerealiseerd moeten zijn.

1.2 De Ketendoelarchitectuur

De Ketendoelarchitectuur, inclusief deze Verdieping, bestrijken de semantische en de technische laag van het raamwerk. Die begrenzing is niet haarscherp. De KDA en de Verdieping stellen wel eisen aan de juridische en organisatie laag. Ook agenderen we vanuit de KDA vraagstukken die op de juridische en/of organisatie laag beantwoord moeten worden.

De KDA richt zich daarmee op het "leidingwerk" voor het uitwisselen van informatie tussen de organisaties die samenwerken in en met de strafrechtketen.



Figuur 1 KDA ten opzichte van de Strafrechtketenarchitectuur geplot op het EIF-Raamwerk

1.3 Keten Businessarchitectuur

De keten-businessarchitectuur van de strafrechtketen is voornamelijk de invulling van de organisatie laag. Met uiteraard een sterke verbinding naar de juridische laag en de semantische laag.

De afspraken over verantwoordelijkheden, processen, diensten, afspraken over kwaliteit en informatie-uitwisseling zijn hier belangrijke onderwerpen. De juridische en organisatorische interoperabiliteit is aan juristen, materiedeskundigen, procesdeskundigen, organisatiekundigen, etc. Oneerbiedig gezegd de "business". De SRK-AR is daar niet leidend, zij is daar dienend, ordenend en adviserend. De SRK-AR doet dat o.a. door de inzet van ketenregiearchitecten en het ondersteunen en adviseren van programma's en projecten. Het bereik van de SRK-AR is daarmee groter dan de scope van de KDA. Zie de vastgestelde notitie "positionering SRK-AR" [PAR].

[1] The new European Interoperability Framework | ISA² (europa.eu)

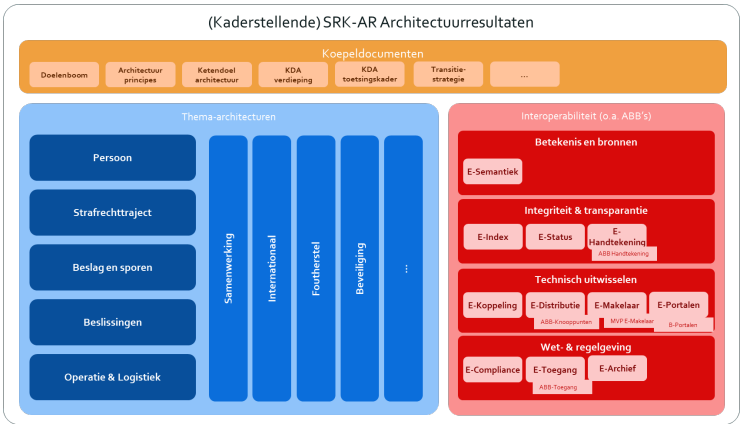
Producten in dit domein zijn niet allemaal SRK-AR producten. Dit domein omvat o.a.:
- leidende principes Digitalisering Strafrechtketen van het BKB/OGB [LPD];
- procesbeschrijvingen (Werk@Wijzer [W@W]) en dienstbeschrijvingen;
- SRK-AR Ketendoelenboom;
- SRK-AR Architectuurprincipes;
- Architecturen welke zijn ontwikkeld in het kader van programma's als Forensisch onderzoek, Multimedia, ZSM, etc.;
- Transitiestrategie SRK-AR.

De businessarchitectuur zal zich in stappen ontwikkelen en ordenen. Enerzijds zijn er bestaande architectuurproducten die keten breed ontsloten moeten gaan worden. Anderzijds zal de businessarchitectuur zich, gestuurd door business- en beleidsdoelstellingen en just-in-time, moeten ontwikkelen. SRK-AR, projecten en programma's leveren daar een bijdrage aan.

1.4 Productstructuur onder KDA

Naast de KDA en de Verdieping is in juni 2021 het toetsingskader KDA gepubliceerd. Het toetsingskader is bedoeld als handreiking en toetsinstrument voor projecten. Het toetsingskader gaat dieper en gedetailleerder in op de KDA. Waar in de KDA en de Verdieping het "waarom" en "wat" centraal staan, gaat het toetsingskader meer over het "hoe".

De KDA en de Verdieping zijn de koepeldocumenten voor de semantiek en techniek laag. De SRK-AR hanteert onderstaande productstructuur voor haar kader stellende architectuurproducten binnen de scope van de KDA.



Figuur 3 Productstructuur kaderstellende producten KDA

De blauwe producten zijn thema-architecturen die een verdieping geven op de semantische laag. De rode producten zijn architectuurproducten voor de technische laag. Deze zijn gegroepeerd rond de clusters van de ketencommunicatievoorzieningen. Zie hiervoor paragraaf 6.3 "Samenhang".

Voorbeelden van deze laatste zijn architectuurbouwblokken (ABB):
- ABB Handtekening (Integriteit & transparantie);
- ABB Portalen (Technisch uitwisselen);
- ABB Knooppunten (Technisch uitwisselen);
- ABB Toegang (Wet & Regelgeving);
- E-Makelaar MVP (Technisch uitwisselen).

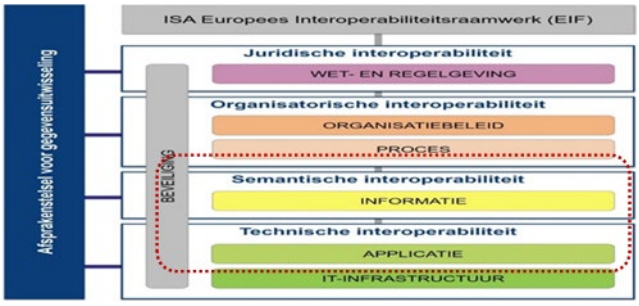
De komende jaren zullen deze architectuurproducten worden ontwikkeld. Het programma Ketenvoorzieningen zal een bijdrage leveren aan het ontwikkelen van architectuurproducten voor de ketencommunicatievoorzieningen.
De prioriteiten voor uitwerking worden gestuurd door de beleids- en digitaliseringsdoelen.

1.5 ASTRA

De ASTRA-website, één van de dochters van de NORA, is de ontsluiting van de architectuur van de strafrechtketen. Alle genoemde architectuurproducten en documenten zijn te vinden op de ASTRA-website.

1.6 Nieuwe versie EIF-Raamwerk

Het EIF-Raamwerk heeft t.o.v. KDA 1.0 een nieuwe vereenvoudigde indeling gekregen.



Figuur 4 Oude EIF-Raamwerk zoals gebruikt in KDA 1.0

In de nieuwe versie, zie Figuur 1, is de onderverdeling van de organisatie laag en de technische laag verdwenen ten opzichte van het model in KDA 1.0, zie Figuur 4.
Dit maakt voor het bereik van de KDA en de Verdieping geen verschil. Zij het dat de KDA en de Verdieping voor het onderwerp IT-Infrastructuur geen uitspraken doen. Hiervoor wordt aangesloten bij de kaders van JenV en het Rijk.

Kerngedachten Ketendoelarchitectuur

Rechtsstatelijkheid en digitale datasoevereiniteit[2]

Rechtsstatelijke verhoudingen en de daarmee gepaard gaande autonomie met sterke checks en balances[3] zijn kenmerkend voor de SRK. Deze komen voort uit onze staatsinrichting, de grondwet, en zijn vertaald in wetgeving zoals het wetboek van Strafvordering, de Politiewet, de wet op de Rechtelijke Organisatie, etc. Het Opdrachtgeversberaad (OGB) heeft dit vastgelegd in de Leidende Principes Digitalisering [LPD] en de SRK-AR heeft dit uitgewerkt in het eerste architectuurprincipe Rechtsstatelijkheid.

De leidende principes en het principe van Rechtsstatelijkheid leiden tot een gedistribueerd IV-Landschap dat de autonomie respecteert, met minimale koppeling tussen de processen, organisaties en IV. Waarbij om de digitale datasoevereiniteit te waarborgen de implementatiekeuze is gemaakt om gegevens op meerdere plaatsen op te slaan. Het laat ook de ruimte voor ketenpartners om de eigen IV naar eigen inzicht in te richten. Een IV-Landschap dat, zoals de OGB-portefeuillehouder Architectuur het formuleert, "als het ware een 'spiegel' dient te zijn van het juridisch stelsel. De informatievoorziening mag geen afhankelijkheden of voorzieningen creëren die strijdig zijn met dat juridische stelsel." Bij de te stellen eisen aan de informatievoorziening is onderscheid te maken naar fases in het proces (vb. vervolging, berechting en ten uitvoerlegging) als ook zaakinhoud en ondersteuning (vb. dossierinzage, biometrische voorziening, identiteit justitiabele en digitale handtekening).

Het gedistribueerde landschap waarbij gegevens op meerdere plaatsen voorkomen stelt eisen aan het kunnen traceren van die informatie om integriteit en authenticiteit te waarborgen. In de memorie van toelichting op de Wet digitale Processtukken Strafvordering 2014 [MDP] wordt gesteld dat het onderscheid tussen origineel en kopie van een document (of informatie) in de digitale wereld onwerkbaar is. De nadruk moet liggen op de traceerbaarheid en onweerlegbaarheid van informatie als ook van (fysieke) bewijsmiddelen. Geconcretiseerd in de begrippen digitale bewaarketen en digitale bewerkingsketen[4]. Wat op zijn beurt weer eisen stelt aan helderheid over verantwoordelijkheden van de ketenpartners.

De rode draad door al deze kenmerken is dat er wel wederzijdse verplichtingen en afhankelijkheden zijn tussen de ketenpartners. Er is op deze onderwerpen geen sprake van een gezamenlijke ketenverantwoordelijkheid. Iedere ketenpartner heeft de verantwoordelijkheid om bij te dragen zodat de keten goed kan functioneren.

Keteninformatisering

Informatisering in een keten is anders dan in een organisatie en kan ook niet gezien worden als de optelsom van de verschillende organisaties. Bij keteninformatisering staat communicatie tussen functionarissen en/of organisaties centraal, in plaats van (gezamenlijke) registratie[5]. De KDA onderkent daarom interactiepatronen om communicatie te duiden. In de keten concurreren keten- en netwerksamenwerking (de horizontale krachten) met organisatiedoelstellingen en -hiërarchie (de verticale krachten). Daar komt bij dat in de keten niemand de "baas" is. [NORA Katern: Ketens de Baas, KDB].

Zoals gesteld zijn er in de strafrechtketen wederzijdse afhankelijkheden en verplichtingen. Geen van de organisaties kan zonder de informatie van de ander. En alleen gezamenlijk kan het "product" van de keten geleverd worden [VIK].
Om de informatievoorziening te richten en te sturen zijn afspraken nodig. Onderlinge afspraken om interoperabel met elkaar te zijn. Interoperabiliteit is "de capaciteit van (soevereine) organisaties om te kunnen samenwerken gericht op het bereiken van gezamenlijke doelen". Interoperabiliteit is daarmee een voorwaarde voor het realiseren van business- en digitaliseringsdoelstellingen en ambities.
De KDA richt zich op interoperabiliteit op de niveaus van semantiek en techniek. De KDA agendeert vraagstukken die op de bovenste lagen (juridisch en organisatorisch) beantwoord moeten worden en stelt ook (vorm)eisen aan deze lagen om daarmee congruent te kunnen zijn.

Figuur 5 Scope KDA i.r.t. EIF

[2] We volgen hier de definitie uit het "Advies borgen digitale soevereiniteit SRK" [BDS]: "complete control over stored and processed data and also the independent decision on who is permitted to have access to it". Zie ook [GAIA].
[3] staatsrecht-systeem waarbij overheidsbevoegdheden over verschillende organen worden verspreid en ieder orgaan bij de uitoefening van zijn bevoegdheden verantwoording verschuldigd is aan een ander orgaan.
[4] Voor definities zie paragraaf 3.2 bladzijde 13.
[5] Deze stelling sluit een gezamenlijke registratie niet uit. Denk hierbij o.a. aan de Strafrechtketen Database voor de leidende administratieve identiteit. Grote terughoudendheid is echter wel geboden.

Gegevenslogistiek in de keten

De Ketendoelarchitectuur (KDA) richt zich op de informatievoorziening (afspraken, processen, mensen, middelen) om de communicatie tussen ketenpartners te ondersteunen.

Het mantra geeft uitdrukking hier aan.

> Mantra SRK-AR
> De strafrechtketen kan digitaal, betrouwbaar, veilig en eenvoudig gegevens over personen, 'zaken'[6], beslissingen en bewijsmiddelen uitwisselen. Zo zijn deze gegevens vanuit ieder gewenst perspectief, binnen en buiten de keten tijdig en volledig beschikbaar, voor iedereen die ze nodig heeft en mag gebruiken, om te kunnen handelen, beslissen, leren, besturen en verantwoorden.

Transitiestrategie: Continu verbeteren

In een keten met grote dynamiek en grote zelfstandigheid van de organisaties past een architectuur die zich kenmerkt als bestemmingsplan, dat richting geeft aan mogelijke initiatieven gecombineerd met een toetsingskader dat, vergelijkbaar met een bouwbesluit, eisen stelt aan de realisatie. Ten slotte is toezicht nodig. Toezicht op naleving en verbetering van gemaakte afspraken. Toezicht dat duidelijk maakt waar concessies worden gedaan aan de interoperabiliteitseisen, consessies die op een later moment gerepareerd moeten worden. Zo wordt de spiraal van het afnemend aanpassings- en ontwikkelvermogen doorbroken.

Deze transitiestrategie vraagt een meerjaren doorkijk van behoeftestellingen gebaseerd op business- en beleidsdoelstellingen en de KDA interoperabiliteitsdoelstellingen. Geconcretiseerd in een portfolioproces voor realisatie binnen een jaar op basis van een ketenjaarplan met daarin ook benodigde resources en financiering. Een (portfolio)proces waarin business- en beleidsdoelstellingen, behoeften en de voorwaardelijke KDA interoperabiliteitsdoelstellingen gebalanceerd worden, evenals organisatie- en ketenbelangen en hun prioriteiten. Naarmate de interoperabiliteit toeneemt zijn de organisaties losser gekoppeld en krijgen organisatie daarmee meer ruimte voor de eigen dynamiek
Om de interoperabiliteit te ondersteunen zijn afspraken, standaarden en (soms gezamenlijke) ICT-voorzieningen nodig, vormgegeven in Ketencommunicatievoorzieningen (KCV'en). Tevens vormen deze de ankerpunten voor kennis en ondersteuning in de keten.

Positionering KDA, way-of-thinking, way-of-working

De KDA heeft als scope, de semantische en technische interoperabiliteit, de gegevenslogistiek. Dat heeft een aantal redenen:

1) De volledige architectuur voor de keten is groter. De juridische en organisatorische interoperabiliteit is aan juristen, materie- en organisatiedeskundigen. Oneerbiedig gezegd de "business". De SRK-AR is daar niet leidend maar dienend, ordenend en adviserend;
2) Een volledig en gedetailleerd ontwerp vooraf werkt niet, zeker niet in een keten. De omvang van de strafrechtketen is te groot en het bijbehorend debat om tot overeenstemming te komen duurt te lang. Dat terwijl er actuele vraagstukken liggen. De SRK-AR streeft naar net genoeg architectuur op het juiste moment, waarbij wordt aangesloten op lopende en aankomende ontwikkelingen en doelstellingen.
3) Op het terrein van gegevenslogistiek zijn veel verbeteringen noodzakelijk en wenselijk. Hetzij vanuit het oogpunt van herstel, hetzij als "enabler" voor verbeteringen in de "business".

Voorgaande impliceert:

- De noodzaak om afstemming tussen business (juridisch, beleid en uitvoering), Portfolioraad en SRK-AR structureel te organiseren zowel inhoudelijk als m.b.t. het portfolio;
- Dat de businessarchitectuur zich in stappen zal ontwikkelen, gestuurd door business- en beleidsdoelstellingen en met behulp van projecten en programma's. De SRK-AR draagt daaraan bij, o.a. met inzet van ketenregiearchitecten. Het bereik van de SRK-AR is groter dan de scope van de KDA. Zie de vastgestelde notitie "positionering SRK-AR" [PAR].
- Voor later gebruik dienen architectuurproducten vastgelegd en beschikbaar te zijn voor de keten.

Voorwaarden voor werken met architectuur

De Ketendoelarchitectuur is onderdeel van een palet aan stuurmiddelen om de doelen van de strafrechtketen te bereiken. Een onderdeel dat in samenhang gerealiseerd moet worden. In de Verdieping wordt op verschillende plaatsen gepleit voor het inrichten van overleggen en processen om samenhang en congruentie tussen de lagen te realiseren. Alsook voor processen en ondersteuning om stapsgewijs te verbeteren (transitie).
Het is niet aan de SRK-AR om dit te ontwerpen en te bepalen. We brengen daarom de volgende onderwerpen graag in bij de inrichting van het Duurzaam Digitaal Stelsel (DDS):

- Organiseren van "businesstafels" voor bespreken juridische en organisatievraagstukken voorzien van een constante bezetting. Te onderscheiden naar strategisch, tactisch en operationeel niveau;
- Inrichten dan wel versterken van processen voor het bepalen van lange- en kortetermijndoelstellingen. Ketenbreed en voortbouwend op o.a. de huidige

[6] De zaak bestaat niet, net zoals het dossier. Dat maakt het zo dringend om verschillend geordende informatie over organisatiegrenzen heen te kunnen relateren. Streven naar een eenduidige definitie van zaak of dossier voor iedereen is een kansloze missie.

portfolioprocessen. Inclusief vraagarticulatie voor de KCV'en;
- Inrichten van operationele ondersteuning voor projecten, programma's en beheer. De "nutsbedrijven" zoals genoemd in de transitiestrategie;
- Inrichten van toezicht op het naleven van afspraken.

3. Rechtsstatelijkheid en digitale datasoevereiniteit

Rechtsstatelijke verhoudingen, voortkomend uit onze staatsinrichting, de grondwet, en vertaalt in wetgeving zoals het wetboek van Strafvordering, de Politiewet, de wet op de Rechtelijke Organisatie, etc., en de daarmee gepaard gaande autonomie van de afzonderlijke organisaties, zijn kenmerkend voor de strafrechtketen.
Het Opdrachtgeversberaad (OGB) heeft dit vastgelegd in de Leidende Principes Digitalisering [LPD] en de SRK-AR heeft dit uitgewerkt in het eerste architectuurprincipe Rechtsstatelijkheid.

De leidende principes en het principe van Rechtsstatelijkheid leiden tot een gedistribueerd IV-Landschap dat de autonomie respecteert, met minimale koppeling tussen de processen, organisaties en IV. Waarbij om de digitale datasoevereiniteit te waarborgen de implementatiekeuze is gemaakt om gegevens op meerdere plaatsen op te slaan. Een IV-Landschap dat, zoals de OGB-portefeuillehouder Architectuur het formuleert, "als het ware een 'spiegel' dient te zijn van het juridisch stelsel. De informatievoorziening mag geen afhankelijkheden of voorzieningen creëren die strijdig zijn met dat juridische stelsel". Bij de te stellen eisen aan de informatievoorziening is het noodzakelijk om kritisch te kijken waar onderscheid is te maken naar fases in het proces (vb. vervolging, berechting en ten uitvoerlegging) alsook het onderscheid tussen zaakinhoud en ondersteuning (vb. dossierinzage, biometrische voorziening, identiteit justitiabele en digitale handtekening).

Kenmerken van de strafrechtketen zijn ook 'bewijsbaarheid' en 'vertrouwelijkheid'. Daarvoor moet te allen tijde aantoonbaar zijn dat informatie integer en authentiek is. De informatie die door de strafrechtketen 'stroomt' moet te traceren en te controleren zijn. De nadruk op traceren en controleren vindt zijn bron in de memorie van toelichting op de Wet digitale Processtukken Strafvordering 2014 [KDA blz. 33]. In de toelichting wordt gesteld dat in de digitale wereld het onderscheid tussen origineel en kopie van een document (of informatie) onwerkbaar is. De nadruk moet liggen op de traceerbaarheid en onweerlegbaarheid van informatie. Geconcretiseerd in de begrippen bewerkingsketen en bewaarketen.

Het derde kenmerk is de eigenstandige verantwoordelijkheid voor het afleggen van verantwoording met betrekking tot gegevensbescherming (o.a. AVG, WPG, WJSG), archivering en informatiebeveiliging (compliance).

Enerzijds is er de zelfstandigheid en autonomie, anderzijds zijn er wel wederzijdse afhankelijkheden tussen de ketenpartners. Er is op deze onderwerpen echter geen sprake van een gezamenlijke ketenverantwoordelijkheid. Iedere ketenpartner heeft de verantwoordelijkheid om bij te dragen zodat de keten goed kan functioneren.

Voorgaande kenmerken vragen een kritische actualisering van gevleugelde uitspraken als "eenmalig opslaan, meervoudig gebruiken", "halen bij de bron" en "scheiden proces en inhoud". In dit hoofdstuk gaan we hier dieper op in.

De KDA beperkt zich weliswaar tot de lagen informatie en applicatie uit het EIF-Raamwerk[7]. Omdat de semantische en technische lagen congruent moeten zijn met de juridische en organisatorische lagen stelt de KDA wel (vorm)eisen aan deze lagen. De KDA agendeert vraagstukken die op de bovenste lagen (juridisch en organisatorisch) beantwoord moeten worden. Denk hierbij aan de gevolgen van persoonsverwisseling of bewaartermijnenproblematiek. Ook stelt de KDA (vorm)eisen aan deze lagen om daarmee congruent te kunnen zijn. Zie de paragrafen over verantwoordelijkheden.

Informatieobject
In dit hoofdstuk gebruiken we de term informatieobject om een betekenisvolle eenheid van gegevens aan te duiden. De SRK-AR bedoelt daarmee een op zichzelf staande eenheid gegevens.

[7] Europees Interoperabiliteits Raamwerk

De drager kan papier, gesproken of gedigitaliseerd zijn, ongeacht de presentatievorm en of het origineel of een "kopie" is. Het kan een 'digital born' document zijn, een multimediabestand (beeld en/of geluid), een gestructureerd bericht, (gescand) papier, telefoongesprek, mail, etc. Het kan ook een dossier zijn met daarin meerdere documenten. Voor de begripsvorming en narratieve doeleinden gebruikt de SRK-AR hier bewust het abstracte begrip "informatieobject" omdat het woord document in de praktijk veelal met een tekstdocument in PDF of Word wordt geassocieerd. In hoofdstuk 5 Informatiemodel, krijgt informatieobject een meer precieze betekenis.

In dit hoofdstuk maken we voor de leesbaarheid geen scherp onderscheid tussen gegevens en informatie. Bij verdere analyse en duiding is het onderscheid wel relevant. Gegevens (data) zijn feiten of symbolen en worden pas informatie als ze betekenis, praktisch nut of relevante nieuwswaarde hebben voor de ontvanger. Voor de leesbaarheid laten we ook het woord informatieproduct buiten beschouwing. In hoofdstuk 5 Informatiemodel brengen we de nodige nuances aan.

3.1 Rechtsstatelijkheid

Recht doen aan de rechtsstatelijke verhoudingen vereist allereerst dat verantwoordelijkheden duidelijk zijn. Dat is makkelijker gezegd dan gedaan. In de praktijk zijn er gewoontes en afspraken die geïnterpreteerd worden als juridisch gegrond maar ontstaan zijn uit "zo doen we het altijd" en pragmatische keuzes. Het is nodig dergelijke praktijken te formaliseren en waar nodig te herzien naar aanleiding van digitaal werken. Bedenk wel dat deze afspraken en ingesleten gewoontes ook de basis zijn voor het vertrouwen in elkaars werkwijze.

Met architectuurprincipe "Dienstoriëntatie" respecteren we de autonomie van de ketenpartner, tegelijkertijd dwingt dit principe tot het expliciteren van verantwoordelijkheden en de bijbehorende kwaliteitseisen tussen ketenpartners in de samenwerking[8]. Bovendien is deze duidelijkheid voorwaardelijk voor het aanwijzen van bronnen voor informatieobjecten. Zie ook werk@wijzer [W@W].

Bij het analyseren en beschrijven van diensten en processen dienen allereerst juridische verantwoordelijkheden te worden geëxpliciteerd. De basis hiervoor is o.a. wet- en regelgeving (zoals WvSv, WJSG, WPG), mandaatbesluiten, instellingsbesluiten. Hierbij dienen organisatie, organisatieonderdeel en functionaris te worden onderscheiden.

> Een voorbeeld:
> DJI (organisatie) heeft de verantwoordelijkheid voor het gevangeniswezen. Echter de directeur in de PI (=functionaris) ontvangt de Last tot ten uitvoerlegging (WvSv art. 6.2.1)
> Voor het beoordelen van toerekeningsvatbaarheid kan de rechter een gedragsdeskundige (een functionaris, WvSv, art. 51i) benoemen. Veelal in dienst of verbonden aan het NIFP (een organisatieonderdeel van DJI).
>
> Zie ook "De verdachte in de ketens" par. 4.1 [VIK], en "Jegens en Wegens" par. 2.5 [JEW].

Waar wet en regelgeving ruimte bieden voor verdere invulling of wellicht zelfs onderling schuren[9] dienen aanvullende afspraken te worden gemaakt of aan de wetgever te worden voorgelegd. De wijze van besluitvorming, zowel juridische als organisatorisch dient nader uitgewerkt uit te worden en mee genomen te worden in de inrichting van het Duurzaam Digitaal Stelsel (DDS).

In de praktijk en bij het inrichten van organisaties worden werkzaamheden, en daarmee bevoegdheden vaak uitbesteed of overgedragen (taakoverheveling). Ook deze attributie, mandatering of delegatie dienen expliciet gemaakt te worden.
We noemen dit in termen van RACI het onderscheid tussen aansprakelijk (accountable) en uitvoeringsverantwoordelijk (responsible)[10]. De aansprakelijkheid is niet over te dragen, anders dan bij wetgeving (v.b. wet USB of Wet SenB) of instellingsbesluit. Overigens valt de verantwoordelijkheid voor de inhoud van een informatieobject nooit over te dragen. Die is en blijft bij de "steller". Een ander kan de gestelde inhoud wel verwerpen of verzoeken te corrigeren.

Het overdragen van verantwoordelijkheid kent het Droste-effect (recursie). Uitbestede werkzaamheden worden (deels) verder overgedragen of gemandateerd. Onder uitbesteden of overgedragen werkzaamheden en verantwoordelijkheden liggen aanvullende mandaat- en delegatiebesluiten[11] of dienstverleningsovereenkomsten.

Wellicht ten overvloede: bij het expliciteren van verantwoordelijkheden moet een duidelijk onderscheid worden gemaakt tussen de bedrijfsdiensten en de ondersteunende informatie/ICT-diensten. In hoofdstuk 3.5 Verantwoordelijkheden is dit verder uitgewerkt.

3.2 Digitale datasoevereiniteit

Rechtsstatelijkheid vereist voldoende en onafhankelijk zeggenschap[12] over de data die relevant is voor een onafhankelijk oordeel: datasoevereiniteit [BDS].

Tegelijkertijd volgt uit diezelfde rechtsstatelijkheid en het strafrechtproces dat de onafhankelijke partijen informatieobjecten aan elkaar moeten kunnen overdragen of delen.

Dat stelt eisen aan de overdracht en het delen. Het stelt ook eisen aan het proces waarin een informatieobject tot stand is gekomen: wie heeft het waargenomen/besloten, wie heeft het vastgelegd, wie is ervoor verantwoordelijk, hoe zijn

[8] Verantwoordelijkheden en bevoegdheden vertalen zich veelal rechtstreeks in diensten. Diensten kennen ook een fijnere granulariteit. Merk op dat we spreken over diensten tussen organisaties, waar de wetgever veelal over de functionaris(type) spreekt.
[9] Voor voorbeelden zie "De verdachte in de digitale bak" [VIB] en het rapport "knelpunten en breukvlakken in de SRK". [KEB]
[10] Het RACI-model is een organisatorisch begrip. Het is geen vervanging voor de staatsrechtelijke juridische begrippen mandateren en delegeren. Het RACI-model volgt daarop.
[11] Mandateren en delegeren hier conform het spraakgebruik / van "De Algemene Wet Bestuursrecht, i.h.b. titel 10 geeft formelere en striktere definities". Zie ook Bijlage 3: Attributie, mandateren en delegeren.
[12] Het betreft hier zeggenschap bezien vanuit de zelfstandigheid en verantwoordelijkheid van de organisatie. Verderop heeft zeggenschap betrekking op doelbinding.

integriteit en authenticiteit gewaarborgd? Tenslotte moet duidelijk zijn welke zeggenschap verstrekker en ontvanger hebben over het gedeelde of overgedragen informatieobject: wie mag het waarom met welk doel gebruiken.

Een voorbeeld:
Welke eisen stelt de Rechtspraak aan het omzetten van een multimedia- bestand, van een onbekend formaat naar een in de keten geaccepteerd formaat, zodat het multimediabestand standhoudt bij de rechter? Is er een vervangingsbesluit nodig?
Het gaat niet alleen om de conversie, maar ook wie is daarvoor geautoriseerd, de betrouwbaarheid van de conversie, de herleidbaarheid tussen origineel en de geconverteerde versie (traceerbaar met behulp van een bewerkingsketen).

Zoals we geleerd hebben bij het tot stand komen van de gekwalificeerde digitale handtekening gaat het niet alleen om de techniek van het plaatsen van een handtekening. Het gaat ook om de wijze waarop de autorisatie en identificatie van de ondertekenaar tot stand komen en de maatregelen die zijn getroffen om onrechtmatig tekenen te voorkomen. Het is uiteindelijk aan de Rechtspraak om te beoordelen of de handtekening standhoudt als bewijsmiddel. Zo sprak de Raad van State zich in 2019 nog uit over het proces van het zetten van een handtekening bij de Rechtspraak.

Het voorbeeld maakt duidelijk dat het introduceren van nieuwe digitale toepassingen in het strafrechtproces deels een zoektocht is. Veel kan van tevoren worden bedacht en/of vastgelegd zijn in de wet en regelgeving. Soms moet er gehandeld worden zodat er, bijvoorbeeld door een proefproces, een onafhankelijk rechterlijk oordeel komt.

Bij het toenemend gebruik van digitale technieken zullen de onderlinge waarborgen in de strafrechtketen aanvullend of zelfs opnieuw moeten worden vormgegeven. Het eerdergenoemde vertrouwen, gebaseerd op afspraken en ingesleten gewoontes uit het papieren tijdperk, dient opnieuw opgebouwd te worden. Nieuwe waarborgen moeten zorgen dat tussen ketenpartijen uitgewisselde informatieobjecten bruikbaar blijven bij de uitvoering van ieders wettelijk voorgeschreven taken.

☞ Daarom dienen partijen samen de eisen te formuleren waaraan de informatieobjecten moeten voldoen die ze van elkaar ontvangen, zodat het bij de ontvanger bruikbaar is onder het recht.

Een voorbeeld:
In de papieren wereld is afgesproken dat bij het overdragen van een document aan de Rechtspraak de pagina's doorlopend zijn genummerd en dat de OvJ kopieën van een handtekening voorziet. Doel hiervan is de compleetheid en authenticiteit te waarborgen.

Dit is één-op-één te automatiseren. In de digitale wereld is het denkbaar dat een digitale handtekening op het document en het valideren daarvan bij ontvangst volstaat om compleetheid en authenticiteit te waarborgen.

Het betreft met name het waarborgen van de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit (BIVA[13]) bij de verwerking en uitwisseling van informatieobjecten. Deze eisen beperken zich, waar nodig, niet tot het moment van overdracht of uitwisseling. Een eis kan ook betrekking hebben op een moment/ stap in het interne proces van een ketenpartner.

De BIVA-eisen zijn (zowel organisatorisch/procesmatig als IV/ICT technisch):
- Beschikbaarheid van de data – erbij kunnen als dat nodig is;
- Integriteit van de data – dat niets is gewijzigd, toegevoegd, verdwenen of achtergehouden;
- Vertrouwelijkheid van de data – alleen toegang als gemachtigd;
- Authenticiteit van de data – is wat het beweert te zijn, vastgelegd door persoon/organisatie op het tijdstip zoals aangegeven.

Begrippen bewaarketen en bewerkingsketen

Geïnspireerd door het begrippenpaar chain-of-custody en chain-of-evidence uit het forensische onderzoek om onweerlegbaarheid te waarborgen, gebruikt de SRK-AR het begrippenpaar bewaarketen en bewerkingsketen voor het volgen van digitale informatieobjecten. Binnen de KDA gebruiken we de begrippen als volgt:

Bewaarketen (logistiek)
Deze ketting beschrijft alle personen die tijdens het onderzoekstraject verantwoordelijk zijn geweest voor het informatieobject.
Kort gezegd: wie heeft het onder zijn/haar hoede gehad ongeacht of de persoon er iets mee gedaan heeft. Dus ook de ontvanger of transportdienst vallen hieronder.

Bewerkingsketen
Deze ketting beschrijft de verrichte handelingen aan het te onderzoeken object en de verkregen resultaten.

[13] BIV is een acroniem uit het domein Informatiebeveiliging en staat voor beschikbaarheid, integriteit, vertrouwelijkheid. Speciaal voor de strafrechtketen voegt de KDA daar de 'A' van authenticiteit aan toe ook omdat dit niet altijd als onderdeel van integriteit wordt beschouwd.

Kort gezegd: wat is door wie met het informatieobject gedaan en wat is het resultaat.

Samenhang
Deze twee ketens zijn samen nodig voor het inzicht om de integriteit en authenticiteit te kunnen beoordelen. Daarbij moet ook de samenhang tussen zowel het origineel als kopieën en afleidingen (vb. samenvatting, bericht) inzichtelijk zijn.

☞ Ten slotte zijn in het kader van grondslag en doelbinding afspraken over de zeggenschap over informatieobjecten nodig. Vragen die beantwoord moeten worden zijn: wie mag wat doen met een informatieobject dat gedeeld of overgedragen is? Mag de ontvanger vrijelijk beschikken over een ontvangen informatieobject of is het gebruik beperkt? Mag de ontvanger de informatieobjecten verder verstrekken? Wat zijn de bewaar- en vernietigingstermijnen? Kan de verstrekker het verstrekken ongedaan maken? Zijn er beperkingen in tijd of door andere gebeurtenissen (vb. het seponeren van een zaak)?
In paragraaf 3.5.3 "Perspectief: gegevensbescherming" staan we hier nogmaals bij stil.

Ketenpartners die informatie willen ontvangen maken met de voor de levering verantwoordelijke organisatie afspraken over de leveringsvoorwaarden[14] (implicatie van het principe Dienstoriëntatie). Een belangrijke voorwaarde is de grondslag/doelbinding op basis waarvan een ketenpartner het informatieobject opvraagt en gaat gebruiken voor het uitvoeren van een taak of het nemen van een beslissing. Het verkregen informatieobject mag alleen hiervoor gebruikt worden en mag niet worden gewijzigd. Daarnaast mag het informatieobject worden opgeslagen voor archivering en het afleggen van verantwoording over de gebruikte informatieobjecten bij de uitgevoerde taak of de genomen beslissing. Een verkregen informatieobject mag in principe niet zomaar worden doorgeleverd aan andere organisaties, tenzij hier een juridische basis en afgesproken condities voor zijn. Indien wordt doorgeleverd, zonder de bevoegdheid, bijvoorbeeld omdat het handig is, is sprake van ongecontroleerd rondpompen waardoor onduidelijk wordt wie verantwoordelijk is voor de kwaliteit, actualiteit en inhoud van het informatieobject en bijbehorende zeggenschap. Bovendien is dit strijdig met de wetgeving betreffende gegevensbescherming.

Een voorbeeld:
De rechter ontvangt een reclasseringsadvies van de OvJ als een van de processtukken. Voor de rechter is de OvJ de "bron" en is dat informatieobject het origineel.

Feitelijk is het een kopie want de OvJ behoudt zijn exemplaar. Het is zelfs een kopie van een kopie. Want de OvJ heeft een exemplaar, een kopie, van het advies van de reclasseringsambtenaar gekregen. Voor de OvJ is de reclasseringsambtenaar de bron.

De reclasseringsambtenaar heeft het "echte origineel".

Een nuancering van voorgaande is op zijn plaats. Er zijn gegevensverzamelingen in de keten waarbij we uitgaan van eenmalige registratie. Dat zijn met name verzamelingen die de unieke identificatie van personen, objecten, etc. voor alle ketenpartners ondersteunen. Het meest bekende voorbeeld is de gegevensverzameling voor de leidende administratieve identiteit (SKDB). Andere verzamelingen zijn de Juridische Documentatie, administratie forensisch en/of in beslag genomen materiaal.

Digitale datasoevereiniteit gaat niet alleen om de onafhankelijkheid en waarborg tussen de ketenpartners. Digitale datasoevereiniteit speelt ook een grote rol bij dataopslag en/of -verwerking buiten Nederland, het gebruik van de Cloud. En binnen de Cloud discussie het onderscheid tussen binnen en buiten de EU. Er is een JenV afwegingskader. Verschillende ketenpartners bepalen op dit moment hun positie ten opzichte van de Cloud. Dat is de eigenstandige bevoegdheid (en verantwoordelijkheid) van de ketenorganisatie waarbij ze acteren binnen de voor hen geldende wettelijke kaders en voldoen aan afgesproken BIVA-eisen.

3.3 Implicaties

Voorgaande leidt tot een gedistribueerde keten-IV die autonomie respecteert, met minimale koppeling tussen de processen, organisaties en IV.
Informatieobjecten kunnen zich op meerdere plaatsen bevinden, gekopieerd worden. Dat stelt eisen aan het kunnen traceren van die informatie om integriteit, authenticiteit en vertrouwelijkheid te waarborgen. Wat op zijn beurt weer eisen stelt aan helderheid over verantwoordelijkheden. Zonder heldere verantwoordelijkheden op juridisch en organisatieniveau kan keteninformatievoorziening geen betrouwbare afspiegeling daarvan vormen.

In de volgende twee paragrafen gaan we in op het traceren van informatieobjecten en verantwoordelijkheden.

[14] Het gaat zowel om de kwaliteit van de dienstverlening (Quality of Service), zoals tijdigheid, beschikbaarheid, etc. als om de aansluitvoorwaarden waaronder de afnemer van de dienst gebruik mag maken.

3.4 Traceren van informatieobjecten

In het gedistribueerde landschap vindt verspreiding gecontroleerd plaats om integriteit, authenticiteit en vertrouwelijkheid te kunnen waarborgen. Vanuit informatieperspectief zijn de bewerkingsketen en bewaarketen de bouwstenen hiervoor. In feite gaan we informatieobjecten vergelijkbaar behandelen zoals dat bij forensisch onderzoek van bijv. een DNA-monster gebeurt.

! Conceptueel is het uitgangspunt dat iedere bewerking van een "informatieobject" en de transformaties, vb. afschrift of samenvatting, de gemaakte kopieën en verschijningsvormen (vb. tekst, beeld, document of bericht) en hun onderlinge relaties uniek worden geïdentificeerd en dat ieder exemplaar wordt voorzien van een handtekening of waarmerk. Op deze wijze ontstaat informatiekundig zicht op hoe een informatieobject, als onderdeel van een dossier, door de keten is gegaan: wanneer welke bewerkingen en transformaties zijn toegepast door wie, en wie wanneer welk exemplaar heeft ontvangen. Door de overdrachtsmomenten te expliciteren is duidelijk wie de zeggenschap heeft over het informatieobject. Op deze wijze ontstaat de benodigde traceerbaarheid en onweerlegbaarheid van informatieobjecten

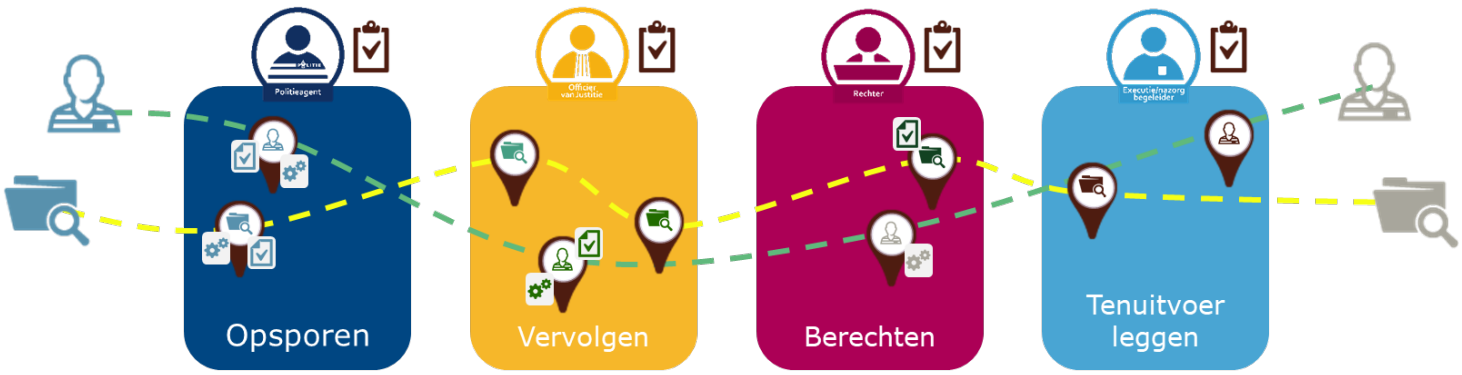
! Het hiervoor beschreven concept is ideaaltypisch. Zowel technisch als organisatorisch zijn er beperkingen, dan wel is een 100% gesloten track & trace voor alle informatie-uitwisseling "overkill". Het gaat om het denken in termen van traceerbaarheid en het versterken van BIVA eisen. Merk ook op dat we hier spreken over informatielogistiek: het kunnen aantonen dat voldaan wordt aan de afgesproken BIVA eisen. We hebben het hier dus niet over het juridische, inhoudelijke proces. Dat laatste is mensenwerk.

Met behulp van dit concept kan ook het spoor met zijn vertakkingen terug gevolgd worden. De hiervoor besproken bewaar- en bewerkingsketen zijn bij uitstek ook het vehikel om in geval van wijziging van of aanvulling op het originele informatieobject de afnemende partijen hierover te informeren. Dit vraagt uiteraard nadere afspraken.

Deze benadering concretiseert ook het uitgangspunt "archive by design" in de visie over duurzaam informatiebeheer. De visie op Digitaal Archiveren [VDA] is maart 2020 vastgesteld door het OGB.

Om informatiekundig te kunnen redeneren over origineel, kopie, bewerkingen is er een metamodel ontwikkeld. Dit wordt behandeld in hoofdstuk 5.

Zoals gesteld zijn de hiervoor beschreven concepten ideaaltypisch. De implementatie van waarborgen voor integriteit en authenticiteit zal een combinatie zijn van organisatorische en technische maatregelen, ondersteund met ketencommunicatievoorzieningen. Zie verder paragraaf 7.2 "Integriteit, traceerbaarheid en transparantie".



Figuur 6 Illustratie van het volgen van persoonsgegevens en digitale processtukken

3.5 Verantwoordelijkheden

In het spraakgebruik is het woord "bron" veel gebruikt. Soms duidt het begrip "bron" op een IT-oplossing soms de verantwoordelijke organisatie of functionaris waarbij vaak nog onduidelijk blijft of het de verantwoordelijkheid voor de inhoud of het verstrekken betreft. Reden voor veel spraakverwarring. Achter het begrip "bron" verschuilt zich veelal de vraag naar een verantwoordelijkheid.

De kern is verantwoordelijkheid, waarbij we het begrip verantwoordelijkheid verder moeten ontrafelen. Bedoelen we met de "bron" de functionaris of organisatie die juridisch verantwoordelijk is voor de inhoud? Wie juridisch verantwoordelijk is voor het verstrekken of het technisch beschikbaar stellen? Bij wie het organisatorisch is belegd? Of bedoelen we tussen welke applicaties we de informatieobjecten uitwisselen?

In deze paragraaf werken we dit uit. We staan eerst stil bij de te onderscheiden soorten verantwoordelijkheden vanuit

businessperspectief (juridisch en organisatorisch) en daarna bij informatieperspectief (semantisch en technisch). We zullen zien dat het begrip bron beperkt moet worden tot de technische laag. De bril waarmee we hier kijken is die van een informatiekundige.

In paragraaf 3.6 "Van bevoegdheden naar verantwoordelijkheden naar informatiebehoeften" geven we een eerste handreiking om gestructureerd hierover te kunnen redeneren.

In deze paragraaf blijven we zoveel mogelijk beschrijvend. In hoofdstuk 5 "Informatiemodel" definiëren we de formele terminologie om hier over te redeneren.

3.5.1 Dienstoriëntatie en procesanalyse

Gezien het sterke juridische karakter van de keten en het principe van rechtsstatelijkheid gaat de ketendoelarchitectuur uit van het expliciteren van bevoegdheden en verantwoordelijkheden, ongeacht of deze voortkomen uit wet- en regelgeving of onderlinge afspraken. Het vehikel om dit te expliciteren en te beschrijven is dienstoriëntatie in combinatie met procesanalyses. Daarmee wordt duidelijk wie waarvan is en meer: welke diensten worden door wie geleverd en onder welke condities en kwaliteitsafspraken. Zie KDA 1.0 voor uitgebreide toelichting op dienstoriëntatie [KDA].

De SRK-AR ziet dienstoriëntatie en procesanalyse als twee elkaar verrijkende denkwijzen, met bijbehorende analyse- en modelleringsmethoden. Waarbij dienstoriëntatie bijdraagt aan het scherp krijgen van ontkoppelpunten en het onderkennen van bevoegdheden, terwijl procesanalyse en -ontwerp helpt bij het expliciteren van bevoegdheden en het waarborgen van operationele samenhang.

N.B. Het concept dienstoriëntatie is van toepassing op iedere laag van het EIF-Raamwerk. Ook bij het begrip dienst dienen we ons steeds af te vragen wat het perspectief is en wat de laag is waarop we spreken.

3.5.2 Perspectief: business

Er is altijd sprake van een bevoegdheid met daaruit voortvloeiende taken en verantwoordelijkheden. Om die taak (dienst) uit te voeren zijn inkomende informatieobjecten nodig, worden nieuwe informatieobjecten gecreëerd en worden er (aangepaste) informatieobjecten beschikbaar gesteld aan anderen.

Dit is natuurlijk te kort door de bocht. Want dit is een informatiekundige bril. Voor het uitvoeren van een taak zijn mensen (medewerkers, verzoekers, etc.), overleg, gebouwen, samenwerking, onderzoek, beslissingen en nog veel meer nodig om een taak uit te voeren. Het resultaat van wat mensen in hun business taak (dienst) doen – een besluit nemen, een beoordeling uitvoeren, een justitiabele vervoeren, een ontsnapping waarnemen, etc., wordt veelal vastgelegd in informatieobjecten. De KDA gaat over informatieobjecten en dan nog altijd aanvullend. Immers mensen overleggen en beslissen en niet alles wat daarbij van belang is, is digitaal.

De-kort-door-de-bocht-formulering maakt duidelijk dat het raadplegen, creëren en beschikbaar stellen van informatieobjecten onlosmakelijk hoort bij het uitoefenen van "business" taken, bevoegdheden en verantwoordelijkheden. Klinkt als een open deur, maar toch. Diezelfde formulering maakt onderscheid tussen binnenkomend, creatie en uitgaand. Verduidelijking aan de hand van een voorbeeld.

PV Verhoor (PV) door een bevoegd agent.

Als een agent een verdachte verhoort dan legt hij het gesprek vast in een proces-verbaal. De agent die het PV opstelt is verantwoordelijk voor de inhoud en hij/zij tekent daarvoor, alsmede de verhoorde. De verhoorde levert zijn/haar verhaal (*binnenkomend*). De politie *creëert de inhoud* van het informatieobject. Op enig moment wordt het PV door de agent/politie verstrekt aan de OvJ (*uitgaand*). Dat uitgaande PV/informatieobject is een "kopie", want de politie en ook de verhoorde hebben een exemplaar. Wat is nu origineel?

Met deze verstrekking gaat ook de zeggenschap over de kopie van het PV mee van de Politie naar de OvJ (*inkomend*). De OvJ mag de inhoud niet wijzigen, zij heeft wel de zeggenschap over het PV, d.w.z. aan wie het wordt verstrekt en of het aan de rechter wordt aangeboden (nemen beslissing, is *creëren*). De overwegingen en aantekening van de OvJ voor haar/zijn beslissing legt deze vast (*creëren*).
De OvJ biedt het PV aan de rechter (*uitgaand*), of niet (*niet uitgaand*). Het aanbieden van het PV is een uiting van de OvJ beslissing, echter zonder zijn eigen aantekeningen mee te geven.
Ook nu is een "kopie" van de inhoud uitgaand, met echter een andere betekenis, aangeboden en ondertekend door de OvJ. Is er nu sprake van een kopie of een nieuw informatieobject?

In het spraakgebruik ziet de OvJ de agent/politie als bron van het PV. De rechter ziet de OvJ als de "bron", immers de OvJ heeft besloten het aan te bieden en de rechter neemt geen stukken van de Politie in ontvangst. De inhoud blijft de verantwoordelijkheid van de agent. De rechter heeft nu de zeggenschap over het PV en beslist aan wie het verstrekt wordt en of het toegelaten of afgewezen wordt als processtuk.

Het voorbeeld maakt een aantal zaken duidelijk.

1) er is verschil tussen verantwoordelijkheid voor het creëren van de inhoud en voor het verstrekken.
2) dat wat als bron wordt gezien is afhankelijk van het standpunt: is het standpunt van de afnemer/ontvanger of van de verstrekker?
3) het verschil origineel en kopie behoeft nadere duiding.
4) wat intern wordt gecreëerd is niet altijd één-op-één gelijk aan wat naar buiten gaat.
5) bron is in het spraakgebruik een verwarrend begrip gezien de verschillende betekenissen (inhoud of van wie je het krijgt) en perspectieven.

Degene die een informatieobject creëert is verantwoordelijk voor de inhoud, dat die inhoud overeenkomt met de, gecreëerde of waargenomen, werkelijkheid en het voldoen aan de benodigde kwaliteitseisen die voor de taak voorkomen uit de BIVA-afspraken.

☞ Alleen degene die heeft gecreëerd heeft het recht dit te herroepen - daarmee ontstaat een nieuwe (gecreëerde of waargenomen) werkelijkheid, die wordt geuit in een nieuw informatieobject dat wordt ondertekend en de vorige "vervangt" / "opvolgt" of aanvult middels een addendum. Ook moet duidelijk worden gemaakt wat met de vorige versie kan of moet gebeuren[15]. Merk op dat wijziging van een informatieobject het gevolg is van een handeling in een proces of dienst. Waarover dus ook afspraken nodig zijn.

Informatie op maat
In het kader van gegevensbescherming kan het noodzakelijk zijn om onderdelen van een informatieobject niet te communiceren.

Geconcretiseerd in een voorbeeld: het is ongewenst dat gegevens van een anonieme getuige bij de verdachte terecht komen. Er zijn informatieobjecten (bijvoorbeeld PV Verhoor) waar die gegevens in staan. Bij een vonnis doen zich vergelijkbare vraagstukken voor. Is voor het innen van een boete het hele vonnis noodzakelijk of kan een uittreksel volstaan?

De vraag die moet worden beantwoord: wie inhoudelijk verantwoordelijk is voor het transformeren van een dergelijk informatieobject. Er ontstaat in feite een nieuw informatieobject (een uittreksel, of beperkt afschrift o.i.d.) wat inhoudelijk voor het verstrekkingsdoel wel juridische toereikend moet zijn op basis van het origineel. En wat is de juridische status van het nieuwe informatieobject?

? Dit vraagstuk is nog onvoldoende uitgewerkt. Duidelijk is al wel dat er niet één antwoord is dat voor alle situaties van toepassing is. Vragen die thuis horen op de juridische tafel.

Het voorbeeld van het PV maakt duidelijk dat er onderscheid is tussen wie verantwoordelijk is voor de inhoud, wie verantwoordelijk is voor de verstrekking[16] aan wie en welke gevolgen dat heeft voor de bijbehorende zeggenschap. Dit wordt in hoge mate bepaald door de context waarin het informatieobject wordt gebruikt. In de strafrechtketen komt het vaak voor dat degene die juridisch verantwoordelijk is voor het verstrekken van een informatieobject niet dezelfde is als degene die verantwoordelijk is voor de inhoud. Zie het voorbeeld en de verantwoordelijkheid van de OvJ om een vonnis uitgesproken door de rechter te verstrekken aan de Minister t.b.v. de ten uitvoerlegging.

☞ We onderkennen dus twee typen rollen:

1) de inhoudsverantwoordelijke;
2) de verstrekkingsverantwoordelijke.

Vaak vallen de verantwoordelijkheden voor inhoud en verstrekking samen. Uit deze voorbeelden moge blijken dat dat in de strafrechtketen geen vanzelfsprekendheid is.

Merk op dat met het verstrekken veelal een verantwoordelijkheid wordt overgedragen en in ieder geval een verwerkingsverantwoordelijkheid ontstaat bij de ontvanger. Het juridisch moment van verstrekken valt niet altijd samen met het moment waarop een informatieobject, fysiek of digitaal, wordt gekopieerd.

Zelf doen of uitbesteden

Naast onderscheid tussen de verantwoordelijkheid voor inhoud en verstrekking is het onderscheid tussen zelf doen of uitbesteden van belang.

Uitbesteden of taakoverheveling komt veel voor. In de huidige praktijk blijft dit vaak impliciet met alle verwarring en ongewenste afhankelijkheden tot gevolg.

☞ We maken daarom, conform het RACI- of RASCI-model, onderscheid tussen aansprakelijk (accountable) en uitvoeringsverantwoordelijk (responsible).

Aansprakelijk kan er maar één zijn. Aansprakelijkheid kan niet worden overgedragen. Met uitbesteden wordt de uitvoerende organisatie of functionaris uitvoeringsverantwoordelijk. Degene die aansprakelijk is dient toezicht te blijven houden op uitbestede of overgedragen taken / werkzaamheden. Dergelijk overdrachten, en de wijze (gemandateerd, gedelegeerd of

[15] Merk op dat wijzigingen, correcties juridisch zeer complex kunnen zijn. Zie ook de Verdachte in de digitale bak [VIB]

[16] We gebruiken op deze laag het woord verstrekken omdat dat een juridische connotatie heeft. Op de semantische laag spreken we van beschikbaar stellen.

geattribueerd) waarop dienen expliciet gemaakt te worden en liggen vast in overeenkomsten.

Gebeurtenissen en wijzigingen

Als er een gebeurtenis is, vb. "een overplaatsing van een justitiabele", "een intrekking van een getuigenverklaring", die tot gevolg heeft dat de inhoud van een eerder verstrekt informatieobject "wijzigt", dient er een nieuw informatieobject gecreëerd te worden door degene die verantwoordelijk is voor de inhoud, waarbij de status van het voorgaande informatieobject wijzigt of een addendum krijgt. Dat vervolgens naar de relevante ketenpartners wordt gecommuniceerd. Hoe? Dat is beschreven in 4.1 Interactiepatronen.

Let op: het niet toelaten van een PV in de terechtzitting door de rechter verandert de inhoud niet. Het is een beslissing (o.b.v. art 359 WvSv) van de rechter, een nieuw besluit dus, die een uitspraak doet over het toelaten van het betreffende PV in een bepaalde zaak. Het is dan niet aan de inhoudelijk verantwoordelijke om dit te communiceren.

Andersom geredeneerd: als de rechter een processtuk accepteert en de inhoud daarvan bekrachtigt met het vonnis verandert de zeggingskracht van dat processtuk waardoor het als bewijs kan dienen in een andere zaak. Bekendmaking van beslissingen met zo'n effect is dan ook noodzakelijk.

3.5.3 Perspectief: gegevensbescherming

In de Strafrechtketen worden (bijzondere) persoonsgegevens verwerkt. Verwerking van persoonsgegevens valt onder de AVG (EU-verordening 2016/679). Voor de verwerking van bijzondere persoonsgegevens in het kader van de openbare orde en veiligheid of opsporing geldt EU-verordening 2016/680, binnen Nederland nader ingevuld met de WPG en WJSG.

Het 'lekken van' bijzondere persoonsgegevens kan een grote impact hebben op de levenssfeer van de betrokkene. Daarom geldt voor het verwerken van bijzondere persoonsgegevens een verbod, tenzij in wetgeving anders is bepaald (een 'uitzondering op'-regel).

Dit maakt dat voor de verwerking van bijzondere persoonsgegevens op voorhand beoordeeld moet worden of dit mag en welke eisen aan die verwerking gesteld worden. Daarom is een Data Protection Impact Assessment (DPIA)/ GegevensbeschermingsEffectBeoordeling (GEB) vaak verplicht. Tijdens die impactanalyse wordt beoordeeld onder welke wettelijke bepaling gegevens verwerkt worden, welk risico bij de verwerking kan optreden en welke maatregelen de risico's doen verkleinen.

Een Data Protection Impact Assessment (DPIA) is vaak verplicht. Voer deze vroegtijdig uit.

Voor iedere verstrekking/ verwerking van persoonsgegevens (d.w.z. inzien, beschikbaar stellen, verstrekken, overdragen etc.) dient er een grondslag en doelbinding aanwezig te zijn. Zonder deze mogen (bijzondere) persoonsgegevens niet verwerkt worden. In de strafrechtketen is in veel gevallen een grondslag te vinden in de WvSv (op doelbinding), WPG en WJSG. Als dat niet het geval is dan zal de grondslag gezocht moeten worden in andere wetgeving. Dat betekent in voorkomende gevallen dat de verwerking vervolgens onder de AVG valt. Het doel waarvoor de gegevens verwerkt worden, moet in lijn zijn met de grondslag die is bepaald voor de verwerking.

Ketenpartners moeten onderlinge afspraken maken over de grondslag en doelbinding voor uitwisseling van persoonsgegevens in een GegevensleveringsOvereenkomst (GLO). Daarin worden onder andere afspraken gemaakt over onderlinge verantwoordelijkheden en onder welke voorwaarden de persoonsgegevens mogen worden verwerkt. Denk hierbij aan het toepassen van dataminimalisatie (noodzaak, proportionaliteit en subsidiariteit), pseudonimisering, encryptie, bewaartermijnen, toegangsrechten etc. Een ontvangende organisatie dient er bijvoorbeeld voor te zorgen dat de verwerking van een ontvangen informatieobject alleen toegankelijk is voor functionarissen die vanuit hun bevoegdheden invulling geven aan de doelbinding. In voorkomende gevallen vereist de wetgeving (WPG en WJSG) geheimhouding van gegevens.

Afspraken over de doelbinding en grondslag voor het uitwisselen van persoonsgegevens (in informatieobjecten) zijn vastgelegd in een GegevensLeveringsOvereenkomst (GLO).

Een ontvangende organisatie dient ervoor te zorgen dat de verwerking van een ontvangen informatieobject alleen toegankelijk is voor de in de doelbinding aangewezen functionarissen.

Bij gebruik van persoonsgegevens moeten de ketenpartners transparant zijn over de gegevensverwerkingen. (Zie ook 7.4.1 "E-Compliance"). Deze moeten opgenomen zijn in het register van verwerkingen en in het (openbare) privacy statement, zodat betrokkenen weten waarvoor hun persoonsgegevens gebruikt wordt, zodat zij makkelijk hun rechten van betrokkene kunnen uitoefenen.

De verwachting is dat met de vernieuwing (samenvoeging) van de WPG en WJSG de eisen met betrekking tot gegevensbescherming duidelijker worden maar wellicht ook op onderdelen strikter dan nu het geval is.

n.b. De AVG spreekt over organisaties als het gaat om gegevensbescherming. Het WvSv spreekt over functionarissen. Hier ontstaat een juridisch grijs gebied. [VIB]

n.b. Het recht "om vergeten te worden" is in de strafrechtketen nog een weerbarstig juridisch vraagstuk. [VIB].

3.5.4 Perspectief: informatie (en applicatie)

Tot nu keken we naar de juridische en organisatorische verantwoordelijkheden. Op de technische laag komt het begrip bron van pas. De locatie die is aangewezen voor het verkrijgen en beschikbaar stellen van informatieobjecten.

Op de semantische laag wijzen we de logische locatie aan van informatieobjecten. Op deze laag spreken we volgens de semantiek van de keten. Degene die verantwoordelijk is voor de inhoud is ook verantwoordelijk voor de ontsluiting van de door hem gecreëerde informatieobjecten voor ketenpartners.

Zoals we eerder zagen hoeft het aan de keten bekendgemaakte informatieobject wat betreft structuur niet één-op-één identiek te zijn aan het eigen interne informatieobject. Er kunnen delen weggelaten zijn omdat deze voor de keten niet relevant zijn. Ook kunnen informatieobjecten worden samengevoegd om ze voor de keten zinvol te maken.
De plaats waar een informatieobject is te verkrijgen noemen we de bronlocatie[17]. Waarbij het goed mogelijk is dat de aangewezen bronlocatie verschilt per afnemer/ontvanger. Zie het voorbeeld van het PV.

Op het niveau van de bron kunnen keuzes gemaakt worden hoe informatieobjecten beschikbaar gesteld worden. Beperkt verstrekken zich tot inzien, is het een kopie (op papier of digitaal) die ter hand is gesteld of is het een geautoriseerde verwijzing naar een andere bron?

De houder van de bronlocatie is verantwoordelijk voor beschikbaarheid, snelheid, beveiliging, toegangsverlening, etc. Deze rol kan samenvallen met de eerder behandelde rollen van inhoud- en verstrekkingsverantwoordelijke. Dat hoeft zeker niet. Een voorbeeld hiervan is het ontsluiten van justitiële documentatie door de Justitiële Informatiedienst (Justid). Noch de inhoudsverantwoordelijke (rechter) noch de verstrekkingsverantwoordelijke (OvJ) zijn de aangewezen bron voor de justitiële documentatie. Die ligt bij de minister.

Een voorbeeld:
DJI is vanuit businessperspectief verantwoordelijk voor het verstrekken van detentiegegevens (vb. verlof van een TBS-gedetineerde) aan de burgemeester. Een deel van die gegevens is afkomstig van DJI, een deel van het OM en het ZM, namelijk de voorwaarden voor het verlof. De applicatie (Injus) en toegang daarvoor zijn in beheer bij de Justitiële Informatiedienst. DJI is aansprakelijk voor het tijdig en juist informeren van de burgemeester, de Justitiële Informatiedienst is uitvoeringsverantwoordelijk: het tijdig en correct beschikbaar stellen.

DJI heeft in het huidige landschap technische beperkingen die het onmogelijk maken een aaneengesloten detentietraject aan de Justitiële Informatiedienst (Justid) beschikbaar te stellen. Afgesproken is dat Justid, conform regels die DJI heeft opgesteld, hiervoor zorgt. Justid creëert hiermee het informatieobject voor de keten.

Er is een DVO tussen DJI en Justid die deze verantwoordelijkheden en afspraken nader vastlegt.

Op de technische laag gaat het om de technische ontsluiting van informatieobjecten. Veel ketenpartners maken gebruik van ICT-dienstverleners voor het hosten van hun applicaties. De technische laag kan nog verder opgedeeld worden naar applicatiecomponenten, dataopslag, etc. Dat voert voor de keten te ver. Hoe een ketenpartner zijn informatievoorziening heeft georganiseerd moet voor de andere ketenpartners transparant zijn.

Ook bij deze verantwoordelijkheden kunnen keuzes worden gemaakt. De verantwoordelijke voor het beschikbaar stellen van informatieobjecten kan deze werkzaamheden zelf doen of uitbesteden. Ook dan ontstaat het onderscheid tussen "aansprakelijkheid" en "uitvoeringsverantwoordelijk" met bijbehorende dienstafspraken en afspraken voor gegevensbescherming.

3.5.5 Resumé

In de paragraaf hebben we laten zien dat er veel verschillende configuraties van verantwoordelijkheden mogelijk zijn. Het begrip bron is in de context van genoemde verantwoordelijkheden ongeschikt om elkaar goed te verstaan.

☞

[17] In USB termen de aangewezen bron

Daarom moeten bij het analyseren van verantwoordelijkheden en bronnen de volgende vragen op business (B) en informatie (I)[18] niveau worden beantwoord:

1. (B) Wie is verantwoordelijk voor de inhoud?
   - Mogelijk te onderscheiden naar aansprakelijk en uitvoeringsverantwoordelijk.
2. (B) Ten behoeve van welk doel is wie verantwoordelijk voor de verstrekking aan wie?
   - Mogelijk te onderscheiden naar aansprakelijk en uitvoeringsverantwoordelijk.
3. (B) Wie is verantwoordelijk voor het op maat maken (vb. uittreksel) of transformeren (vb. tekst naar gestructureerde gegevens) van een informatieobject? En creëert daarmee al dan niet een nieuw informatieobject en wordt verantwoordelijk voor de inhoud. Komt in essentie overeen met de eerste vraag.
4. (B) Welke zeggenschap heeft de ontvanger na het verstrekken van het informatieobject?
5. (I) Wie is verantwoordelijk voor het beschikbaar stellen aan wie?
   - Mogelijk te onderscheiden naar aansprakelijk en uitvoeringsverantwoordelijk.
6. (I) Wie is verantwoordelijk voor het technisch beschikbaar stellen?
   - Mogelijk te onderscheiden naar aansprakelijk en uitvoeringsverantwoordelijk.

3.6 Van bevoegdheden naar verantwoordelijkheden naar informatiebehoeften

In het resumé staat de top-down aanpak met de vraag "wat moet en mag?" centraal.

Grofweg bestaat deze top-down aanpak uit de stappen:
Bepaal op basis van en in deze volgorde Wet- & Regelgeving, organisatiebesluiten, instellingsbesluiten en mandaatregelingen:

- de bestaansreden van een bevoegdheid en bijbehorende verantwoordelijkheid (het waarom);
- waarop de bevoegdheid is gebaseerd (grondslag);
- aan wie (functionaris) de bevoegdheid is toebedeeld (in staatsrechtelijke begrippen);
- wie de gevolgen van de verantwoordelijkheid ondergaat: de bevoegde en verantwoordelijke functionaris en/of organisatie, de betrokkenen (burger, justitiabele, burgemeester, etc.);
- welke eisen gesteld worden aan de uitvoering en/of het resultaat;
- aan wie gemandateerd of gedelegeerd wordt (staatrechtelijk);
- afhankelijkheden van andere verantwoordelijkheden;

De wet- en regelgeving laat ruimte voor beleidskeuzes:

- bepaal welke functionaris, organisatie daadwerkelijk wordt belast met de uitvoering en wie houdt toezicht;
- Wat zijn de eisen mb.t. beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit.

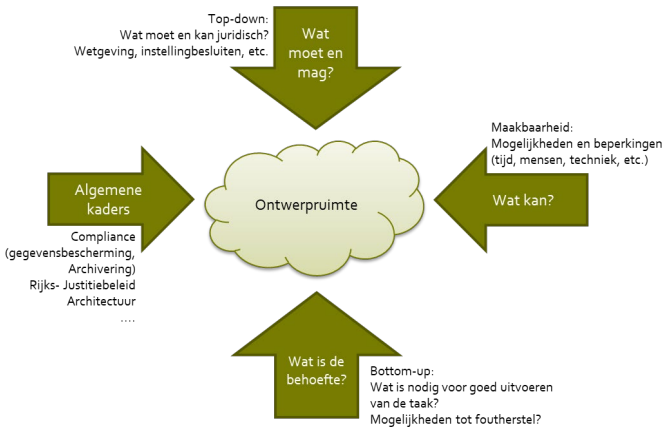
Naast top-down is ook de bottom-up aanpak nodig. Daarin staan de vragen centraal:

- welke informatie heeft de professional nodig om diens taak goed te kunnen uitvoeren?
- aan welke BIVA-Eisen (beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit) moet worden voldaan?

De afweging tussen "nodig" en "mogen" dient aangevuld te worden met de perspectieven:

- Maatregelen t.b.v. gegevensbescherming;
- Compliance-eisen: archivering, verantwoording;
- Veiligheid medewerkers en betrokkenen;
- Kwaliteitsbewaking;
- Architectuur;

Als deze afweging is gemaakt volgt een toets op maakbaarheid en haalbaarheid. Deze krachten gezamenlijk bepalen uiteindelijk de ontwerpruimte.
Het bepalen van de ontwerpruimte van de informatiebehoefte is een iteratief proces. Waarbij bijvoorbeeld technische onmogelijkheden een heroverweging vragen van "wat moet" door bijvoorbeeld de wet aan te laten passen. Evenzo kunnen nieuwe technische mogelijkheden leiden tot andere BIVA-maatregelen. Het is dus zaak om zo snel mogelijk integraal de ontwerpruimte te verkennen.



Door verantwoordelijkheden, processen, diensten en informatieobjecten tegen elkaar uit zetten ontstaat zicht op volledigheid.

[18] Principe uit de USB architectuur

Voorgaande schets van te maken analyses, keuzes en besluiten maakt duidelijk dat deze zich over alle lagen van het EIF-Raamwerk uitstrekken. Dat betekent ook dat verschillende deskundigheden nodig zijn om tot gebalanceerde keuzes te komen. Van juristen tot materie- en procesdeskundigen, van medewerkers tot informatiekundigen.

! Design Thinking[19] biedt een goede werkwijze om iteratief met meerdere disciplines tot de ontwerpruimte te komen.

Deze analyses, afstemming en besluitvorming structureel organiseren zijn voorwaardelijk om succesvol te informatiseren in de keten. Het ontbreken van structurele afstemming en besluitvorming is een bron van veel vertragingen en langlopende discussies. Dit is een van de elementen die in de keten georganiseerd moet worden. Zie ook 4.8 "IV organiseren in de keten".

? De SRK-AR werkt aan een stappenplan en begrippenapparaat voor het maken van deze gelaagde analyses en gezamenlijke begrippen om afstemming te bevorderen. In deze benadering krijgen zowel dienstoriëntatie als procesoriëntatie een plaats.

3.7 Gevleugelde uitdrukkingen herzien

Bij gesprekken over informatiseren in de keten en in projecten worden in discussies vaak oneliners gebruikt. Oneliners die na verloop van tijd voorbijgaan aan de bedoeling, de achterliggende gedachte. Vervolgens leiden deze oneliners, waar eenieder ondertussen zijn eigen interpretatie van heeft, tot verbitterde discussies en niet tot een goed gesprek. In deze paragraaf nuanceert de SRK-AR een aantal veel gebezigde oneliners en voorzien ze van een nieuw versienummer 2.0.

1) "Niet meer rondpompen";
2) "Halen bij de bron";
3) "Eenmalig opslaan, meervoudig gebruiken";
4) "Scheiden proces en informatie".

3.7.1 **"Niet meer rondpompen 2.0"**

Rondpompen is het verspreiden, kopiëren van informatieobjecten naar wie het nodig heeft zonder zich al te veel te bekommeren om informatie op maat, integriteit en authenticiteit. Waardoor (later) blijkt dat iemand over te veel informatie beschikt of over een verouderd informatieobject beschikt of dat de actualiteit van een informatieobject onzeker is. Dan wel dat gegevensbescherming en archiefverplichtingen met voeten getreden worden.

Het adagium "niet meer rondpompen" staat voor de ambitie om op maat te informeren met de zekerheid van integriteit en authenticiteit en verkrijgen van de juiste informatie uit de juiste bron. De informatiebehoefte is leidend o.b.v. een grondslag en doelbinding inclusief de eisen m.b.t. subsidiariteit, proportionaliteit en transparantie. Aangeleverde gegevens worden niet bewerkt, behoudens aanvullende metadatering. Voorkomen van "redundantie" is zeker geen doel op zich[20].

In de KDA is het maken van kopieën noodzakelijkerwijs (datasoevereiniteit, compliance) toegestaan. Informatie komt op meerdere plaatsen terecht. Dit klinkt als rondpompen maar is het niet. Zoals hiervoor beschreven worden strenge eisen gesteld aan "kopiëren". Daardoor zijn informatieobjecten met behulp van de bewaarketen en bewerkingsketen traceerbaar.

3.7.2 **"Halen bij de bron 2.0"**

Het is een gevleugelde uitspraak in de keten: "halen bij de bron". Het oogmerk van halen bij de bron is het verkrijgen van eenduidige informatie zodat er zekerheid is dat men de juiste informatieobjecten verkrijgt van degene die daarvoor verantwoordelijk is.

"Halen bij de bron" heeft tot veel verhitte debatten en miscommunicatie geleid. Ten eerste is niet altijd duidelijk wat met bron bedoeld wordt: Inhoudelijk verantwoordelijk, verantwoordelijk voor het verstrekken, of het technisch beschikbaar stellen, etc. De KDA beperkt het begrip bron tot de technische laag van het EIF-Raamwerk. Zie ook 3.5.4.

Ten tweede wordt "halen bij de bron" vaak geïnterpreteerd als halen van het informatieobject bij diegene die verantwoordelijk is voor de inhoud. Zoals we hebben aangetoond in de paragraaf 3.5 valt de verantwoordelijkheid voor het verstrekken en beschikbaar stellen, ongeacht op welke EIF-Raamwerk laag, niet altijd samen.

In hoofdstuk 3.5 is duidelijk gemaakt dat "halen bij de bron" een degelijke analyse vraagt en dat de verantwoordelijkheden eerst geëxpliciteerd moeten worden voordat we weten wat in een concrete casus de bron is of bronnen zijn. Zonder deze analyse is de kans op misverstanden levensgroot. Daarom een upgrade van "Halen bij de bron" naar 2.0.

[19] Vb. Guido Stompff, Design thinking, Boom

[20] Er is een fundamentele discussie te voeren wanneer er sprake is van redundantie. Immers als een inhoudelijk identiek informatieobject onder een andere verantwoordelijkheid valt met daarbij behorende grondslag en doelbinding is het dan nog wel hetzelfde informatieobject? In hoofdstuk 5 Informatiemodel komen we hier op terug.

! Met "Halen bij de bron 2.0" nodigen we uit om het gesprek over verantwoordelijkheden op het scherpst van de snede te voeren en helder onderscheid te maken tussen de verschillende verantwoordelijkheden en daarna pas over de technische bron te spreken.

3.7.3 "Eenmalig opslaan meervoudig gebruiken 2.0"

Deze veelgehoorde uitspraak, die ook is opgenomen in de EA JenV, is een verkeerd citaat van principes uit de NORA. Het afgeleide principe van NORA stelt "Afnemers wordt niet naar reeds bekende informatie gevraagd" wat vertaald wordt in gezamenlijk gegevensgebruik: "Gegevens worden in beginsel slechts eenmalig verzameld en vervolgens meervoudig bij uitvoering van verschillende wetten gebruikt". Dit voorkomt irritatie bij degene die de gegevens moet aanleveren en het beperkt invoerfouten door niet steeds opnieuw te registreren.

NORA zegt niets over opslaan of kopiëren. Ketenpartners dienen zich te kunnen verantwoorden en hebben een eigen verantwoordelijkheid voor archiveren. (zie de paragrafen Rechtsstatelijkheid en Digitale datasoevereiniteit). Mede daarom zullen informatieobjecten meermalen worden opgeslagen. De leidende principes en de visie en scenario's Digitaal Archiveren sluiten gezamenlijk archiveren uit[21]. [VDA, SDA].

Zoals in paragraaf 3.2 Digitale datasoevereiniteit besproken is zijn er gegevensverzamelingen in de keten waarbij we uitgaan van eenmalige registratie. Denk hierbij aan biometrische kenmerken, de leidende administratieve identiteit (SKDB), in beslaggenomen goederen.

Het meervoudig gebruiken van informatieobjecten voor verschillende wetgeving en doelen aangevuld met de privacy wetgeving (AVG, WPG, WJSG) vraagt binnen de strafrechtketen om een zeer kritische afweging. En kan niet zo letterlijk overgenomen worden. Binnen de strafrechtketen zijn grondslagen en doelbinding essentieel voor de rechten van betrokkenen. Dit moet voorkomen dat persoonsinformatie voor één onderzoek 'toevallig' wordt vastgelegd buiten de context van dat doel (dat onderzoek) en zo wordt verspreid.

! Het is verstandig de uitspraak "eenmalig opslaan, etc." niet meer te gebruiken omdat deze onjuist en verwarrend is. Wel dienen we de oorspronkelijke kern vast te houden "Afnemers wordt niet naar reeds bekende informatie gevraagd". Daarbij hoort dat we die beschikbare informatie ook gebruiken. Een slachtoffer of anonieme getuige moet erop kunnen vertrouwen dat diens toegezegde bescherming bij de noodzakelijke ketenpartners bekend is. Op ketenniveau zijn hiervoor afspraken en voorzieningen nodig, mogelijk zelfs gezamenlijke.

3.7.4 "Scheiden proces en informatie 2.0"

Ook deze oneliner, verzelfstandigd uit een USB-principe, is stof voor verhitte debatten. We brengen enige richtinggevende nuances aan.

Het scheiden van proceslogica van inhoudelijke gegevens is een software-architectuurprincipe. Het principe beoogt door compartimentering software overzichtelijk en onderhoudbaar te houden. Daarnaast biedt compartimentering voordelen voor o.a. performance, geheugengebruik en dataopslag.

Een praktisch voorbeeld hiervan. Het OM (OvJ) biedt de Rechtspraak (rechter) een zeer omvangrijke verzameling processtukken (informatieobjecten) aan. Het in één keer aanbieden van al deze informatieobjecten kan leiden tot verstopping op het netwerk en de systemen van OM en ZM. Daarom is het handig dat het OM de Rechtspraak informeert dat een verzameling processtukken klaar staat, waarna de Rechtspraak kan beslissen de processtukken op een geschikt moment naar zich toe te halen. Het is ook goed denkbaar dat het informeren dat de processtukken klaar staan via een ander kanaal bekend wordt gemaakt dan waar de stukken opgehaald kunnen worden.

Het onderscheid tussen proces en informatie hoort op de technische laag. In de praktijk wordt het principe ook toegepast op de organisatie-laag bij het ontwerp van processen en diensten. Waarbij proces en informatie gescheiden worden en afzonderlijk door twee organisaties aangeboden worden[22].

Schematisch: ketenpartner A doet een verzoek (een stap in een proces) aan ketenpartner B. Het verzoek wordt uitgebracht met minimale informatie waarna ketenpartner B de aanvullende informatie verkrijgt van ketenpartner C.

Het op deze wijze een-op-een doortrekken van een software-architectuurprincipe naar bedrijfsdiensten en -processen kan leiden tot onduidelijkheden in verantwoordelijkheden. Er ontstaat een driehoeksrelatie waarbij onduidelijk wordt wie er verantwoordelijk is voor het samenhangend en volledig informeren van ketenpartner B. Daarnaast is het niet uitgesloten dat tegenstrijdigheden ontstaan tussen de verkregen informatie van ketenpartner A en ketenpartner C. Deze extra afhankelijkheden dragen niet bij aan het

[21] CDD is geen ketenarchief maar een gezamenlijke voorziening waarin ieder ketenpartner zijn archief, als eigen gegevensverzameling, onder eigen beheer heeft.

[22] Een radicale interpretatie van "halen bij de bron" om "rondpompen" te voorkomen. Waarbij de bron degene is die inhoudelijk verantwoordelijk is voor het informatieobject. "Halen bij de bron" en "niet meer rondpompen" zijn hiervoor al genuanceerd.

doelgericht uitvoeren van taken en het verbeteren van de ketensamenwerking en -prestaties.

De KDA sluit toepassing van het principe in ontwerp in processen en diensten op de organisatie laag niet uit. Onder het voorbehoud dat verantwoordelijkheden helder zijn, de samenhang van informatie gewaarborgd is en aan BIVA- en privacy-eisen is voldaan.

Het onderscheid tussen proces en informatie hoort primair op de technische laag.

4. Keteninformatisering

In het vorige hoofdstuk hebben we uitgebreid stil gestaan bij de Rechtsstatelijkheid omdat dit kenmerkend is voor de strafrechtketen en daarmee de basis vormt voor verdere uitwerking van de ketendoelarchitectuur.

Informatisering in een keten is anders dan in een organisatie en kan ook niet gezien worden als de optelsom van de verschillende organisaties. Bij keteninformatisering staat communicatie tussen functionarissen en/of organisaties centraal, in plaats van (gezamenlijke) registratie[23,24]. Om te kunnen communiceren zijn identificatie (nummerstelsels), onderlinge relaties en begrip van elkaars taal van groot belang. [Grijpink, KKB]

In de keten concurreren keten- en netwerksamenwerking (de horizontale krachten) met organisatiedoelstellingen en hiërarchie (de verticale krachten). Daar komt bij dat in de keten niemand de "baas" is. Dat vraagt "Verticaal sturen versus horizontaal verbinden" [NORA, KDB].

Tegelijkertijd is er een wederzijdse afhankelijkheid. Geen van de organisaties kan zonder zowel de inhoudelijke- als de procesinformatie van de ander. En alleen gezamenlijk kan het "product" van de strafrechtketen geleverd worden [VIK].

Om die wederzijdse afhankelijkheden met betrekking tot informatievoorziening te richten en te sturen zijn afspraken nodig. Onderlinge afspraken om interoperabel met elkaar te zijn. Interoperabiliteit is "de capaciteit van (soevereine) organisaties om te kunnen samenwerken gericht op het bereiken van gezamenlijke doelen".[25] Zoals in hoofdstuk 1 is beschreven is interoperabiliteit noodzakelijk op alle lagen van het EIF-Raamwerk, van juridisch tot en met de techniek.

De KDA richt zich op de semantische laag en technische laag van het EIF-Raamwerk. Daarmee richt zij zich op de informatievoorziening om de communicatie tussen ketenpartners te ondersteunen.
Het mantra geeft uitdrukking hier aan. We drukken daarin uit dat het gaat over betrouwbare digitale communicatie en de traceerbaarheid van die informatie zodat de samenhang van informatie gewaarborgd blijft. Het is de richtinggevende visie voor het streven naar de "ideale" informatievoorziening in de keten. Waarbij we ons bewust zijn dat de perfecte eindsituatie nooit zal bestaan. Met het voortschrijden verschuift de horizon. En tussen droom en daad zijn altijd praktische bezwaren.

Mantra: SRK-AR
De strafrechtketen kan digitaal, betrouwbaar, veilig en eenvoudig gegevens over personen, 'zaken', beslissingen en bewijsmiddelen uitwisselen. Zo zijn deze gegevens vanuit ieder gewenst perspectief, binnen en buiten de keten tijdig en volledig beschikbaar, voor iedereen die ze nodig heeft en mag gebruiken, om te kunnen handelen, beslissen, leren, besturen en verantwoorden.

Om de interoperabiliteit te realiseren hebben we in de keten nadere afspraken nodig. In dit hoofdstuk verdiepen we een aantal onderwerpen uit de KDA met betrekking tot keteninformatisering. Onderwerpen die tot discussies leiden in projecten. Het gaat hier bijvoorbeeld om de rol van interactiepatronen, het "dossier", gegevensbescherming, kwaliteitsbewaking, tijdreizen, kwaliteitsbewaking en foutherstel.

Tot slot. Ook keteninformatisering moet georganiseerd worden en daarvoor zet de KDA een aantal uitgangspunten neer. Aangevuld met een begrippen om over gemeenschappelijk, generiek, etc. te kunnen redeneren.

N.B. Keten of netwerk?
Of er sprake is van een strafrechtketen of een strafrechtsnetwerk is in het boek van Wim Borst uitgebreid behandeld [VIK]. Het onderscheid is relevant voor afspraken en samenwerkingsrelaties. Ketenpartners dienen in verschillende ketens en netwerken te kunnen communiceren. De discussie keten of netwerk is vooral een oproep om keuzes breder af te wegen dan het strafrechtproces in enge zin. Voor het vraagstuk van interoperabiliteit op de semantische- en technische laag maakt het uiteindelijk weinig verschil, waardoor de KDA dit onderscheid ook niet maakt in haar uitwerking.

[23] Dat sluit een gezamenlijke registratie niet uit. Denk hierbij o.a. aan de Strafrechtketen Database voor de leidende administratieve identiteit. Grote terughoudendheid is echter wel geboden.

[24] Zoals in het vorige hoofdstuk is betoogd kiest de Strafrechtketen niet voor gezamenlijke registraties, tenzij ...

[25] Conform Europees Interoperabiliteit Framework (EIF). Voor relatie met NORA zie Alignment NORA en EIF - NORA Online

Figuur 7 Interactiepatronen

4.1 Interactiepatronen

Zoals betoogd staat in de keten de communicatie, in het kader van taken en verantwoordelijkheden, tussen organisaties / functionarissen centraal. Daarom zijn in de KDA 1.0 de interactiepatronen geïntroduceerd. Het afspraken-, het vraaggestuurde informatiedeling- en attendering[26]-interactiepatroon. Zie [KDA].

Kort geformuleerd zijn dit de patronen: A en B maken een afspraak en houden beide het vervolg in de gaten tot de afspraak is afgesloten (afsprakenpatroon). C wil iets weten van D of andersom, als de vraag is beantwoord is de dialoog afgelopen, tenzij er een nieuwe vraag wordt gesteld (vraaggestuurde informatiedeling). A deelt aan ieder die het wil en mag weten iets mee en is niet geïnteresseerd wat de ontvanger er mee doet (attendering).

Alle interacties in en met de keten zijn een uiting van één van deze drie patronen. Processen zijn te zien als een aaneenschakeling van interacties en daarmee de interactiepatronen. Indelen in deze patronen helpt om verantwoordelijkheden te expliciteren, diensten te onderkennen en vervolgens te vertalen naar de bijbehorende technische implementatie. Het gekozen interactiepatroon is congruent met de aard van de communicatie.

In gesprekken merkt de SRK-AR dat de interactiepatronen vaak voor technische interactiepatronen, berichtuitwisseling, worden aangezien[27]. Het is van groot belang dit onderscheid scherp te maken.

Om verwarring te beperken gebruiken we in onze documenten voor technische interacties de term uitwisselpatronen.

Het feit dat een bericht technisch correct is afgeleverd bij een andere ketenpartner geeft geen garantie dat een medewerker van die ketenpartner daar actie op gaat nemen. Hiervoor is een bevestiging, bijvoorbeeld via een bericht of per telefoon, nodig. Het zou niet de eerste keer zijn dat daardoor zaken vertraging oplopen of niet de juiste aandacht krijgen.

Als de zekerheid over daadwerkelijk handelen nodig is, is het afsprakenpatroon noodzakelijk.

Het verschil tussen interacties en technische uitwisselpatronen kan ook andersom geïllustreerd worden. Zo kan de start van het afspraken interactiepatroon op technisch niveau beginnen met een technische notificatiebericht waarop de ontvanger een technisch vraagbericht stuurt voor verdere informatie of het ophalen van bijbehorende informatieobjecten. En vervolgens een bevestiging van de afspraak maakt middels een technisch notificatiebericht.

Een paar verduidelijkingen en aanvullingen op de KDA:

4.1.1 Afspraken interactiepatroon

Het interactiepatroon "afspraken" en dienstoriëntatie dragen beide bij aan het expliciteren van verantwoordelijkheden en verzakelijking van de samenwerking.

[26] "Attenderingspatroon" heette in de KDA 1.0 "notificatiepatroon". Het alternatief "kennisgevingspatroon" is afgewezen omdat dit een zeer sterke juridische connotatie heeft. Deze keuze is in lijn met de eerdere USB-besluiten.

[27] Ook bij de implementatie van de ebMS standaard worden bedrijfstransacties vaak verward met transacties die zich op de technische laag bevinden.

Het begrip afspraak moet ruim geïnterpreteerd worden. Ook een formele overdracht van stukken waardoor de ontvanger actie moet gaan nemen voor verdere behandeling (vb. overdracht van een vonnis aan de minister) ziet de KDA als afspraak. Net zo goed als het verzoek om een persoon te vervoeren.

Het afsprakenpatroon kent meerdere mogelijke statussen voor de happy en de crappy flow. Deze statussen zijn allereerst bedoeld om een zorgvuldige analyse te maken. Eén-op-één vertalen van handmatige naar digitale processen kan leiden tot een grote administratieve last die niet in verhouding staat tot het beoogde doel.

☞ Daarom dient per status uit het afsprakenpatroon te worden toegelicht waarom deze status wel/niet expliciet en formeel wordt uitgevoerd en gecommuniceerd en gedigitaliseerd.

Stappen in het afsprakenpatroon, die leiden tot statussen:
Verzoeken: De ene partij (**dienstafnemer**) vraagt aan de andere partij (**dienstverlener**) hem een dienst te verlenen.
Beloven: De dienstverlener belooft de dienst te leveren onder de afgesproken voorwaarden.
Weigeren: de dienstverlener weigert de dienst te leveren.
Uitvoeren: De dienstverlener gaat aan de slag om de beloofde dienst te realiseren.
Verklaren: De dienstverlener verklaart dat hij de dienst heeft gerealiseerd zoals beloofd.
Aanvaarden: De dienstafnemer aanvaardt de geleverde dienst.
Afwijzen: de dienstafnemer wijst de geleverde dienst af.
Herroepen: de dienstverlener en dienstafnemer kunnen op enig moment hun aangegane commitment (b.v. verzoek, belofte, maar ook verklaring of aanvaarding) **herroepen**, zodat b.v. de dienst niet geleverd gaat worden.
Niet nakomen: Ten slotte kunnen afspraken **niet nagekomen** worden.

☞ Wijzigingen in het afsprakenpatroon: ongeacht door wie afspraken gewijzigd of herroepen worden of onderliggende gegevens van de afspraak worden gewijzigd, dienen uitgevoerd te worden met het afsprakenpatroon en niet met het attenderingspatroon.

4.1.2 Vraaggestuurde patroon

Op een vraag volgt altijd een antwoord, mits voldaan aan grondslag en doelbinding. Uiteraard zijn hier afspraken over gemaakt tussen vragensteller en vraagbeantwoorder.

Het vraaggestuurde patroon levert altijd een momentopname op: de gegevens zoals ze op dat moment beschikbaar zijn. Dat wil zeggen dat als de vraag opnieuw wordt gesteld mogelijk een ander antwoord volgt. Het is aan de vragensteller om zich op de hoogte te (laten[28]) stellen van wijzigingen of een antwoord te vergelijken met een eerder verkregen antwoord. Ook kan de vragensteller van verstrekker niet eisen dat deze het antwoord op een eerdere gestelde vraag kan reproduceren. Zie ook paragraaf 4.6 Tijdreizen.

Een nuancering op het voorgaande: als een vragensteller vraagt naar een geïdentificeerd, integer en authentiek/ gewaarmerkt informatieobject dan zal hij/zij uiteraard iedere keer hetzelfde antwoord te krijgen, binnen de normen van bewaartermijnen en archiefwet. Dat er een nieuwe versie beschikbaar is of een aanvulling krijgt de vragensteller niet via dit patroon te weten.

☞ Voor het actief geattendeerd worden op wijzigingen is het Attenderingspatroon aangewezen, tenzij de wijziging betrekking heeft op een afspraak, dan is het Afsprakenpatroon aangewezen.

4.1.3 Attenderingspatroon

☞ Bij het interactiepatroon attendering deelt de signaleerder van een gebeurtenis het optreden van die gebeurtenis mee aan mogelijk geïnteresseerden. De signaleerder ontvangt geen feedback op bedrijfsniveau.

Het attenderingspatroon gaat uit van het mededelen van een gebeurtenis[29]. Een voorbeelduitwerking staat in de VNG afspraken in het kader van common ground.

De attendering bevat genoeg informatie, maar vanuit gegevensbescherming ook niet meer dan dat, om urgentie/relevantie voor de ontvanger te bepalen. Hier is geen algemene regel voor te geven. De ontvanger zal, indien geïnteresseerd, middels het interactiepatroon vraaggestuurd aanvullende, voor hem relevante, informatieobject(en) op maat vragen.

! De inhoud van een attendering is balanceren tussen relevantie, gegevensbescherming, overbodige mededelingen, efficiency, etc.

Een paar voorbeelden
Een attendering "Een gedetineerde is ontsnapt" is weinig behulpzaam want zal leiden tot een veelheid aan vragen: "Wie?", "Waar?", "Wanneer?", etc.

[28] Middels attenderingspatroon

[29] Vergelijkbaar met de bedrijfsgebeurtenis gedreven opzet uit de USB architectuur. Echter in de KDA wordt nader onderscheid gemaakt tussen afspraken en attenderen.

Een attendering "Peter X, geb. d.d., met BSN, wonende te Rotterdam, met volgend signalement en bijgaande foto" is te veel (dataminimalisatie).

De attendering "SKN 123 heeft risicotaxatie 1" is onjuist omdat het een toestand weergeeft en geen gebeurtenis. Beter is "gewijzigde risicotaxatie opgesteld voor SKN 123".

De grondslag en doelbinding voor het ontvangen van attenderingen vindt plaats op het moment van afsluiten van een abonnement, de wens om in kennis gesteld te worden, en niet per afzonderlijke attendering.

Het is aan de ontvanger om toe te zien dat een attendering, of wellicht onderdelen daarvan, bij de juiste persoon terecht komen.

4.2 Dossier

Dit betreft afspraken, juridisch, organisatorisch en informatorisch, over de opbouw van, het overdragen van en de zeggenschap over dossiers, inclusief bijbehorende BIVA afspraken. Er zijn verschillende type dossiers te onderkennen, "het dossier" bestaat immers niet.

? Dit onderwerp dient op korte termijn nader uit gewerkt te worden. Er zijn meerdere werkgroepen actief. Hiervoor zal een document, als onderdeel van de thema-architecturen strafrechttraject logistiek, worden opgeleverd.

4.3 Gegevensbescherming

! Dit betreft het beschermen van persoonsgegevens van slachtoffers [PVS], getuigen, justitiabelen en mogelijk meer betrokkenen zoals advocaten. Hoe te voorkomen dat persoonsgegevens ongewenst gedeeld worden.

? Deze afscherming dient nader uitgewerkt te worden voor alle betrokken personen.

In het kader van slachtoffergegevens zijn meerdere onderzoeken gedaan. De actuele stand is op te vragen bij DGSenB.

4.4 Papier en digitaal, gestructureerd en ongestructureerd

4.4.1 Digital-born

De KDA hanteert het principe "Digitaal is onze taal". De strafrechtketen streeft naar digital-born informatieobjecten die gedeeld kunnen worden zodat overtypen, kopiëren en scannen overbodig worden en waarmee de foutgevoeligheid wordt geminimaliseerd. Machineverwerkbare gegevens dragen bij aan het verminderen van administratieve last.

Tegelijk zal papier niet volledig uitgebannen worden. Dat vereist dat processen en daarmee de KDA ook papieren informatieobjecten moet ondersteunen. Naar de aard van de keten zal ook mondelinge uitwisseling een zeer belangrijk deel uitmaken van het uitwisselen van informatieobjecten.

4.4.2 Gestructureerde gegevens[30]

"Digitaal is onze taal" wordt heel vaak uitgelegd als "alle informatieobjecten moeten 'gestructureerd' zijn". Dit in tegenstelling tot documenten. Documenten die wel een structuur hebben maar niet of beperkt door een computer verwerkbaar zijn.

! De KDA is hier genuanceerd in en spreekt de voorkeur uit voor gestructureerd wat gestructureerd kan en zinnig is, de uiteindelijke keuze is aan de "business".

Overweging hierbij: er zijn informatieobjecten die om uiteenlopende redenen, zoals juridische kaders, verantwoordingsplicht of begrijpelijkheid, niet uiteen gerafeld kunnen worden in gestructureerde gegevens.

Bij gestructureerde gegevens is de wijze waarop de gegevens gepresenteerd worden aan een mens losgekoppeld van de gegevens zelf. Dit betekent dat de presentatie per situatie kan verschillen.

! Dit is echter niet altijd wenselijk of toegestaan. Wil een mens de authenticiteit kunnen verifiëren dan is de combinatie van presentatie en gegevens gelijktijdig nodig. Voorbeeld een beschikking tot voorlopige hechtenis moet voor de verdachte leesbaar en herkenbaar zijn. Een XML-bericht volstaat dan niet.

Om die reden worden soms wettelijke eisen gesteld aan de manier waarop gegevens worden opgemaakt en gepresenteerd. Dit is in de strafrechtelijke context nog vaak het geval. Een uitgeschreven vonnis moet voor burgers en andere betrokkenen herkenbaar zijn als een authentiek document afkomstig van een rechtbank en moet door een rechter ondertekend zijn.

[30] Het onderscheid tussen gestructureerd en ongestructureerd wordt hier grofstoffelijk gebruikt. Bij verdere detaillering is het geen binaire tegenstelling maar een genuanceerde overgang.

Wet- en regelgeving leggen beperkingen op. Tegelijkertijd kan het geen kwaad wetgeving tegen het licht te houden om te bezien of een beperking (nog) noodzakelijk is of anders vorm ingevuld kan worden.

Het structureren van informatieobjecten maakt het beter mogelijk om informatie op maat te leveren[31]. En daarmee te voldoen aan de eisen met betrekking tot gegevensbescherming (dataminimalisatie en substitutie). Een document zoals een vonnis of PV bevat vaak gegevens voor verschillende doeleinden/taken. Niet iedereen heeft alle informatie uit het document voor zijn taak nodig. Het integraal verstrekken is een potentiële bron van informatielekken. Denk aan de problematiek omtrent slachtoffergegevens.

Merk op dat een document en de daaruit afgeleide gestructureerde gegevens verschillende verschijningsvormen zijn met (nu nog) een verschillende juridische status. In hoofdstuk 5 Informatiemodel gaan we hier dieper op in.

4.5 Kwaliteitsbewaking: Forward Control 2.0

Uit de werk@wijzer [W@W]: "Binnen de Uitvoeringsketen Strafrechtelijke Beslissingen werken we volgens het uitgangspunt "forward control". Dit betekent dat iedere ketenpartner verantwoordelijk is voor de kwaliteit, juistheid, volledigheid en tijdigheid van gegevens die deze partner ter beschikking stelt."

In lijn met het betoog "Verantwoordelijkheden" is een nuancering van dit statement nodig. Een verstrekkende verantwoordelijkheid (o.a. tijdigheid, volledigheid) valt niet altijd samen met de verantwoordelijkheid voor de inhoud (juistheid).

! De essentie van het statement beoogt dat we vertrouwen op de deskundigheid en zorgvuldigheid van ketenpartners en dat de ontvangende ketenpartner geen compenserende maatregelen neemt om het werk van de aanleverende ketenpartner over te doen en te controleren. Waarbij het overdoen op langere termijn veelal een corrumperende bijwerking heeft. Het wordt immers "toch wel gecontroleerd".

In de architectuur voor de strafrechtketen nemen we dit uitgangspunt over. We voegen er wel nuanceringen aan toe omdat het uitgangspunt in de praktijk tot taaie discussies leidt.

! Fouten ondergraven het vertrouwen in de democratische rechtsstaat en kunnen ingrijpende gevolgen hebben voor de betrokkenen. Zorgvuldigheid is een essentieel kenmerk van de strafrechtketen. De praktijk laat zien dat mensen en systemen fouten maken en dat zal altijd zo blijven. Blind vertrouwen zonder kwaliteitscontroles, is gezien de impact van fouten, ongewenst.

☞ Op kritieke punten in de keten dienen kwaliteitscontroles te worden ingebouwd. Dit kan op casusniveau (extra check op identiteit bijvoorbeeld), op proces of op systeemniveau. Het is aan ketenpartners om gezamenlijk af te spreken welke kwaliteitscontroles men in de keten inricht.

☞ Eenzijdige compenserende controlemaatregelen, waarbij de ontvangende ketenpartner het werk van de verstrekkende ketenpartner overdoet of controleert buiten de kwaliteitsafspraken om, zijn niet toegestaan.

! Bij het geven van vertrouwen hoort transparantie alsook het aanspreken van elkaar op het beschamen van het vertrouwen.

4.6 Tijdreizen

Welke gegevens waren beschikbaar op het moment van raadplegen of beslissen? En is dat later terug te vinden? Kortom: "Wat wist de professional op dat specifiek moment in tijd?" en wellicht "Wat had de professional kunnen, of wellicht moeten, weten?". Terugkijken in de tijd is nodig voor het afleggen van verantwoording, foutherstel, leren, verbeteren, etc. Het vraagstuk van "tijdreizen".

Tijdreizen toegelicht
Het moment van verstrekken (t) door of raadplegen van een bron bepaalt de informatiepositie van de afnemer. Wat nu als over een week (t+1) dezelfde bron over hetzelfde wordt bevraagd en de bronfeiten zijn veranderd? Dan krijgt de afnemer, in de huidige situatie, andere informatie en is veelal niet meer te zien hoe de informatie op moment (t) was. Dat roept het probleem op: "wat wist je op dat specifieke moment (t) in tijd?". Lastig als je moet verantwoorden op grond van welke informatie een beslissing is genomen. Waarbij ook nog onderscheid gemaakt moet worden tussen de juridische (materiele) en administratieve (formele) stand van zaken[32].

Een voorbeeld: het kan zijn dat persoon N op 1-2-2020 op een zitting veroordeeld is, terwijl dat pas op 7-2-2020 wordt geadministreerd. Als op 6-2-2020 wordt gevraagd

[31] Gestructureerde gegevens, die ook in het document voorkomen, worden vaak metadata genoemd. Dat zijn het echter niet. Het is een andere (deel)representatie van de inhoud.

[32] De ontwerpen van de basisadministraties geven hiervoor aanwijzingen. [CBB]

naar de veroordelingen van N dan is het administratieve antwoord "niet bekend" want de juridische werkelijkheid is nog niet vastgelegd. Als op 8-2, na de vastlegging, de vraag wordt gesteld hoe de stand was op 6-2-2020 zal het antwoord zijn "veroordeeld op 1-2-2020, administratief nog niet want vastgelegd op 7-2-2020.". Waarmee de informatiepositie op 6-2-2020 herleid kan worden. De medewerker kon op 6-2 niet weten dat persoon N veroordeeld was. (tenzij de medewerker bij de zitting op 1-2 was). Voorgaande impliceert dat dezelfde software en autorisaties worden gebruikt. Het gaat niet alleen om de gegevens als ook om de techniek voor ontsluiting.

Zie Historische gegevens en tijdreizen [HGT] voor meer uitleg.

Het overgrote deel van de informatiesystemen in de strafrechtketen is ongeschikt om "terug te gaan in de tijd", laat staan in samenhang over de gehele keten. Het is niet te verwachten dat op afzienbare termijn samenhangend digitaal "tijdreizen" in de strafrechtketen mogelijk is. Als het al mogelijk is om sluitend terug te gaan in de tijd.

☞ Zoals in KDA 1.0 is afgesproken, is het aan de ketenpartner om informatieobjecten voor het afleggen van verantwoording zelf te bewaren. Een ketenpartner kan hiervoor niet leunen op de andere ketenpartner, tenzij hierover nadere dienstverleningsafspraken zijn gemaakt. De aansprakelijkheid blijft bij de ketenpartner die zich moet kunnen verantwoorden.

☞ Populair gezegd: tijdreizen is op ketenniveau (voorlopig) niet mogelijk. Dus: ontwerp informatie (keten)processen vanuit het bewustzijn dat tijdreizen niet mogelijk is en tref voorzieningen om verantwoording af te kunnen leggen. We voorkomen hiermee onnodige complexiteit en respecteren de rechtsstatelijke- en archiefverantwoordelijkheden.

! Voor nieuwe informatiesystemen cq. -toepassingen is het wel aanbevolen om gebeurtenisgedreven[33] te ontwerpen en te ontwikkelen i.p.v. toestandsgericht.

Concreet: baseer administraties dan niet zozeer op toestanden (zoals verdachte, laatste verblijfadres, aanwezig-in-detentie), maar op resultaten van diensten (zoals beoordeling betrokkenheid, verhuizen / verhuizing doorgeven, in detentie nemen, ontsnapping waarnemen, aanwezigheid constateren). Dan is het informatiekundig mogelijk de toestand op een bepaald moment af te leiden, terwijl alle aanleidingen die die toestand tot stand brachten ook beschikbaar en traceerbaar zijn in de administratie.

! Maak alleen, indien vanuit businessperspectief zinvol, onderscheid tussen de materiële en (vb. formele historie.

Materiële historie geeft aan wanneer een verandering is opgetreden in de werkelijkheid.
Formele historie geeft aan wanneer in de administratie een verandering is verwerkt.
Bron: Catalogus BAG [CBB]

☞ (Wettelijke) registers in de strafrechtketen worden gebeurtenisgedreven ingericht en maken onderscheid tussen de materiële en formele historie zodat vastleggingen en wijzingen in tijd te volgen zijn.

4.7 Foutherstel

Een zwakke plek in iedere keten is het herstellen van fouten die zich verspreid hebben door de keten. Ongeacht hoe deze fout, per ongeluk (vb. typefout) of met opzet (vb. identiteitsfraude), is ontstaan. Zolang een fout zich beperkt tot binnen de muren van een organisatie is dit redelijk goed te herstellen. Verlaat het foute gegeven de organisatie en vindt er besmetting plaats bij het handelen van andere organisaties die op grond van die foute informatie handelen, dan is herstel uiterst moeizaam. In het boek "De verdachte in de digitale bak" [VIB] zijn de complicaties bij identiteitsverwisseling t.g.v. fraude of administratieve fouten uitgebreid beschreven.

Voor een betrokkene die in een dergelijke situatie terecht is gekomen, is het herstellen van zo'n fout nauwelijks mogelijk. Het corrigeren op de plaats waar de fout is ontstaan is veelal niet voldoende omdat de fout zich verder in de keten heeft verspreid, met nieuwe fouten tot gevolg. Alleen een bericht sturen met het juiste informatieobject is niet voldoende. Voor het oplossen van dergelijke fouten moeten ketenpartners in gezamenlijkheid afzonderlijke compenserende acties uitvoeren. Zie de casus Ron Kowsoleea, de voorbeelden van de Kafka-brigade [DDK] en het Meldpunt Identiteitsfraude.

☞ Het herstellen van organisatie-overstijgende fouten behoort ook tot de kerntaken van de ketenpartners. Bij het ontwerpen van processen en diensten dient ook het herstel van fouten zoveel mogelijk ontworpen te worden. Dat betreft zowel herstel voor betrokkene, bijvoorbeeld het herstellen van een vonnis op de verkeerde naam, als het corrigeren van bijbehorende administraties.

! De KDA doet geen uitspraak in welke mate dit geautomatiseerd of handmatig moet gebeuren. De vastlegging van een bewerkingsketen en het

[33] Eventsourcing. Zie https://martinfowler.com/eaaDev/EventSourcing.html

afsprakenpatroon kunnen wel faciliteren in de analyse van de "verspreiding" van de fout.

☞ Ketenpartners toetsen aan de hand van simulaties en ketentesten de robuustheid van het herstelvermogen, in het ontwerp en in de praktijk. Afspraken met betrekking tot foutherstel worden opgenomen bij de kwaliteitseisen van de dienstverlening en de aansluitvoorwaarden voor de dienstverlening. Besteedt hierbij speciaal aandacht aan de doorlooptijd om fouten zo snel mogelijk te herstellen.

4.8 IV organiseren in de keten

Organisaties hebben de I-discipline georganiseerd. Van richtend (CIO-office) tot verrichtend (beheer en ontwikkeling). Ook in de keten dient dit georganiseerd te worden. Niet als aparte entiteit, maar als een gezamenlijk verband van de ketenpartners.

4.8.1 Richten: Congruentie tussen lagen

Zoals betoogd in hoofdstuk 3 zijn voor interoperabiliteit afspraken nodig. Afspraken die beginnen op de overlegtafels waar de juridische en organisatie keuzes en behoeften worden bepaald, die vervolgens in samenhang met de informatievoorzieningstafel worden uitgewerkt.
Het inrichten van tafels voor besluitvoorbereiding en beslissen is een voorwaarde om richting te geven aan en prioriteiten te bepalen voor de interoperabiliteit. Zie ook paragraaf 3.6 " Van bevoegdheden naar verantwoordelijkheden naar informatiebehoeften".

4.8.2 Inrichten: lusten en lasten verdelen

Dat de lusten (de baten) bij een andere organisatie vallen dan de organisatie die de lasten (inspanning) levert, is een kenmerkend probleem voor samenwerking in ketens en netwerken. De SRK-AR pleit dan ook voor samenwerkingsgerichte financiering.

! Het moet voor ketenpartners ook financieel aantrekkelijk zijn om mee te werken aan de afspraken. Eventueel door een tijdelijke subsidie om aan te gaan sluiten op de ketenafspraken. Of door een compensatie te geven als de lasten bij een andere ketenpartner vallen dan bij degene die die de lusten heeft.

4.8.3 Inrichten: Samenhang organiseren

Architectuur, informatiemanagement, portfoliomanagement zijn voorwaardelijk om in samenhang te realiseren. Zie ook 8.1 Transitiestrategie (KDA Perspectief).

4.8.4 Verrichten: Nutsbedrijven

De strafrechtketen is slecht in het bewaren van kennis en afspraken op ketenniveau. Wielen worden meerdere keren uitgevonden, afspraken ad-hoc gemaakt zonder ketenbrede afwegingen. De SRK-AR pleit in haar transitiestrategie, hoofdstuk 8, dan ook voor 'nutsbedrijfjes', onder te brengen bij ketenpartners of dienstverleners. 'Nutsbedrijfjes', die projecten, beheer en de ketenpartijen ondersteunen in het komen tot afspraken, die de afstemming organiseren. Tevens verzamelen, ordenen en ontsluiten zij kennis en stellen die beschikbaar voor de ketenpartijen.

4.8.5 Meerdere ketens

Alle organisaties in de strafrechtketen opereren in meer ketens. Denk aan de zorgketen, de migratieketen, de civiele keten, etc. Het is voor de organisaties complicerend tot ondoenlijk om aan uiteenlopende of conflicterende afspraken en standaarden van verschillende ketens te voldoen.

☞ Met het maken van afspraken en standaarden voor de strafrechtketen wordt daarom zoveel mogelijk voldaan aan Europese (o.a. EIF-Raamwerk, E-Codex , Rijks (o.a. NORA, forum Standaardisatie) en JenV afspraken en standaarden. Alleen daar waar het strafrechtketen-specifiek is wordt afgeweken of verbijzonderd.

4.8.6 Verschil in tempo en verantwoordelijkheden

De leidende principes digitalisering strafrechtketen [LPD] gaan uit van zelfbinding van de ketenpartners om aan afspraken en standaarden te voldoen. Dat is dus geen ketenverantwoordelijkheid.

Tegelijkertijd dienen we in de keten rekening te houden met tempoverschillen. Waarbij sommige partners wel en andere nog niet aan de afspraken kunnen voldoen.

☞ Om die verschillen te overbruggen zijn soms tijdelijke (ICT) constructies nodig. Een tijdelijke constructie tussen huidige (status ketenpartner) en gewenste (conform ketenafspraak) situatie is soms nodig. Voor dergelijke tijdelijke constructies ligt de verantwoordelijkheid voor beheer en financiering bij de betreffende ketenpartner. Andere ketenpartners mogen bijspringen in capaciteit of financiën omdat dat de keten als geheel vooruit helpt. Het mag echter geen ketenoplossing worden.

4.8.7 Toezicht op afspraken

Een keten kan niet alleen werken bij de gratie van afspraken. Allereerst dienen deze afspraken voor wie ze nodig heeft duurzaam toegankelijk te zijn en vervolgens dient toegezien te worden op naleving. De praktijk van de afgelopen jaren heeft ons geleerd dat alleen het maken van afspraken niet

voldoende is. Afspraken zijn slecht terug te vinden en worden om uiteenlopende redenen niet nagekomen. Het toezien op en handhaven van afspraken is, vriendelijk gezegd, niet sterk ontwikkeld.

De keten zet nu sterk in op digitaliseren. Dit betekent dat de eisen aan betrouwbaarheid, integriteit, vertrouwelijkheid en authenticiteit van informatieobjecten opnieuw vorm worden gegeven.

Het is daarom van belang om het handhaven en naleven van en toezien op afspraken te versterken. Alleen zo kan het vertrouwen in, door digitalisering, veranderde werkwijzen en technieken opnieuw worden opgebouwd. Het is ook noodzakelijk om de doelstelling van interoperabiliteit te realiseren. Ook uit oogpunt van kosten, beschikbare capaciteit en flexibiliteit is de huidige vrijblijvendheid niet langer mogelijk.
Dat vraagt transparantie, d.w.z. inzicht geven in de stand van zaken en de moed om elkaar aan te spreken.

Ketenpartners verbinden zich door zelfbinding aan gezamenlijk gemaakte afspraken [LPD]. Bij zelfbinding past dat toezicht bij voorkeur met behulp van intercollegiale toetsing en peerreviews worden ingericht. Voor sommige processen en voorzieningen zal een externe toetsing of audit nodig zijn, zoals dat voor de digitale handtekening reeds het geval is.

☞ Ketenafspraken m.b.t. de interoperabiliteit op de lagen informatie en applicatie uit het EIF-Raamwerk zijn van toepassing op bilaterale implementaties tussen ketenpartners.

Ketenafspraken en -voorzieningen staan niet stil. Door zowel technische of organisatorische vernieuwing als uit de praktijk komen voorstellen om ketenvoorzieningen te verbeteren, te vernieuwen of af te schaffen. Er dient een entiteit te zijn die de realisatie bij voortduring toetst op de gestelde (BIVA) eisen. Omdat dit vaak specifieke expertise vraagt is het aan te bevelen dit te beleggen bij entiteiten die hierin zijn gespecialiseerd.

Een voorbeeld: het algoritme dat gebruikt wordt voor het zetten en versleutelen van een digitale handtekening dient met de komst van grotere rekenkracht te worden vervangen om betrouwbaar te blijven. Leveranciers hanteren nu vaak een houdbaarheidstermijn van ca. 5 jaar. Er dient een entiteit te zijn die dergelijke vernieuwing initieert.

4.9 Gemeenschappelijke-, gezamenlijke-, gedeelde-, generieke-, keten-, -voorzieningen

Deze begrippen zorgen voor de nodige spraakverwarring. Onder deze begrippen gaan ten minste 3 dimensies schuil:
1) De reikwijdte van gebruik van de voorziening: publiek, rijk, ministerie, keten, organisatie.
2) Verplicht gebruik en wijze van financiering binnen JenV;
3) De mate van gezamenlijkheid van ICT: delen van ontwerp, techniek, functionaliteit, data;

Ad 1) Om de verwarring te beperken gebruiken we de door de CIO-Raad JenV vastgestelde begrippen:

Begrip	Reikwijdte gebruik	Voorbeeld
Generiek	Overheid- rijksniveau	Digid, E-Herkenning
Gemeen-schappelijk	Ministerie (JenV)	CDD, Jubes
Keten	Ketenspecifiek (vb. SRK, Migratieketen, Jeugd)	CDM SRK
Gedeeld	Tussen 2 of meer organisaties (evt. uit verschillende ketens)	GPS, Biometrie-voorziening

Ad 2) Binnen JenV wordt om verplichting en financiering te duiden, onderscheid gemaakt tussen basisdiensten en gedeelde diensten. Een basisdienst is verplicht voor alle organisaties en iedere organisatie betaalt mee (voorbeeld Justitienet). Een gedeelde dienst is niet verplicht en wordt gefinancierd door de deelnemende afnemers. Bijvoorbeeld de biometrie voorziening voor een aantal partners in de migratie- en strafrechtketen.

Ad 3) Voor de gezamenlijk gebruik van ICT kan ook gekeken worden of gegevens, applicaties, ontwerpen, etc. gedeeld worden. Dit kan variëren van ieder volledig voor zich tot en met één applicatie met "gedeelde data". En allerlei varianten daartussen. Hiervoor is geen formele terminologie afgesproken. Vaak worden ook hier begrippen als generiek en gemeenschappelijk gebruikt.

! Het zal duidelijk zijn dat al deze varianten en begrippen een bron voor misverstanden zijn. Navragen wat wordt bedoeld is noodzakelijk.

Welke variant en combinatie gewenst en mogelijk is, is allereerst gebaseerd op rechtsstatelijkheid en datasoevereiniteit. En heeft vervolgens gevolgen voor de inrichting van governance, financiering etc.

4.10 Informatiebeveiliging

☞ De KDA heeft het bereik tot beveiligingsniveau BBN2, (DepV).
Als een hoger beveiligingsniveau nodig is dienen aanvullende maatregelen getroffen te worden. Getoetst moet worden of de kaders van de KDA hieraan voldoen.

Voor beveiliging wordt waar mogelijk aangesloten op Justitie [KIBV] en Rijks [BIO] afspraken en standaarden.

? Punt van onderzoek: welke specifieke eisen zijn voor de strafrechtketen nodig.

5. Informatiemodel

Twee belangrijke elementen van de Ketendoelarchitectuur zijn 1) het expliciteren van verantwoordelijkheden en 2) het kunnen volgen van informatieobjecten. In pargraaf 3.5 Verantwoordelijkheden *zijn verschillende verantwoordelijkheden beschreven. in paragraaf 3.4 Traceren van informatieobjecten werd er onderscheid gemaakt tussen "origineel", kopie, exemplaar, etc.*

Om over beide onderwerpen te kunnen redeneren zijn begrippen en een model nodig. De KDA vat dit samen onder het informatiemodel. Het informatiemodel is een model voor architecten. Het model beschrijft dus niet de informatieobjecten van de strafrechtketen (personen, aangiften, uitspraak, etc.). Daarvoor is er o.a. het CDM , ook een onderdeel van E-Semantiek.

In dit hoofdstuk lichten wij de begrippen en het model toe. Het model gaat uit van de ideaaltypische concepten zoals beschreven in paragraaf 3.4 "Traceren van informatieobjecten". De waarschuwingen die daar zijn gegeven zijn uiteraard ook voor dit hoofdstuk van toepassing. Het is een conceptuele denkrichting, een groeipad met technische, juridische en organisatorische (on)mogelijkheden.

De doelgroepen van dit hoofdstuk zijn architecten, businessanalisten en informatieanalisten.

5.1 Objecten en hun samenhang

Om gegevens over objecten (personen, dingen of concepten in de werkelijkheid zoals justitiabele Piet en incident "caféruzie bij Lowietje", "Vonnis 123") samenhangend beschikbaar te hebben, moet informatie daarover worden verwerkt via (een aan elkaar gerelateerde set van) informatieobjecten. Verwerking van informatie over die objecten (in de werkelijkheid) zal leiden tot een veelvoud van informatieobjecten op verschillende plaatsen bij verschillende ketenpartijen. Elk van die informatieobjecten bevat gegevens over het te volgen object. Zo zal de naam of het verblijfadres van die ene justitiabele in verschillende informatieobjecten opgenomen zijn. Het kunnen volgen van een object, zoals een persoon of zaak, in de keten uit zich dus door het kunnen volgen van informatieobjecten waarin informatie te vinden is over dat object. Daarvoor is een aantal dingen nodig: objecten moeten worden geïdentificeerd, informatieobjecten met gegevens over die objecten moeten aan elkaar kunnen worden gerelateerd en vanuit verschillende perspectieven bevraagd kunnen worden. Dit sluit aan op de concepten van semantisch web en Linked Data.

Daartoe gaan we als eerste in op wat informatieobjecten zijn. Daarna gaan we in op de samenhang van objecten en traceerbaarheid van exemplaren. Tenslotte benoemen we daaruit voorvloeiende verantwoordelijkheden.

5.2 Informatieobject: de bouwsteen voor gegevensverwerking

5.2.1 Informatieobject

Ten behoeve van samenwerking binnen de SRK moet informatie worden vastgelegd, uitgewisseld en geraadpleegd; hierna aangeduid als gegevensverwerking. Daarbij moet de betekenis en inhoud van die gegevensverwerking duidelijk zijn. Gegevensverwerking gebeurt in termen van betekenisvolle gehelen van gegevens, ieder aangeduid als informatieobject.

Definitie Informatieobject
Een op zichzelf staand geheel van gegevens met een eigen identiteit.

Een informatieobject is een verzameling van gegevens dat als eenheid wordt behandeld. Ieder informatieobject kent een eigen identiteit. Een "eigen identiteit" betekent dat een informatieobject een identificatiekenmerk (nummer of attribuutset) heeft waardoor het te onderscheiden is van andere informatieobjecten. Hiermee kan een gebruiker eenduidig verwijzen naar het informatieobject en kunnen relaties tussen informatieobjecten worden gelegd, waardoor traceerbaarheid mogelijk wordt.

Wat die betekenisvolle eenheid is, is afhankelijk van het doel waarvoor het informatieobject wordt gecreeerd of verwerkt. Als voorbeeld kan dienen de set gegevens die samen de vastgelegde verklaring van een aangever vormen. Voor ieder informatieobject moeten daarom afspraken gemaakt over:

- het doel waarvoor het informatieobject wordt verwerkt;
- de gegevens waaruit het informatieobject bestaat;
- wat de betekenis is van die verzameling gegevens en van de gegevenselementen die er deel van uitmaken.

Merk op dat een informatieobject een gedachteconstructie is. Een informatieobject betreft de betekenisvolle informatie-inhoud, maar heeft nog geen vorm. Inhoud zonder vorm kan in de werkelijkheid niet kan voorkomen. Zie verder 5.2.3.

5.2.2 Informatieobjecttype

Natuurlijk worden er niet voor ieder individueel informatieobject afspraken gemaakt, maar wordt dit voor de klasse van informatieobjecten met overeenkomende eigenschappen gedaan. Zo'n klasse van informatieobjecten wordt aangeduid met *informatieobjecttype*.

Definitie Informatieobjecttype
De klasse van informatieobjecten met overeenkomende eigenschappen.

Een informatieobjecttype definieert de semantiek (inclusief syntax) voor elk informatieobject van dat type, inclusief de gegevenselementen die dat informatieobject bevat. Andersom noemen we een informatieobject van informatieobjecttype X een **instantie** (EN: *instance;* in NL soms ook *vóórkomen*) van informatieobjecttype X. Zo is Informatieobject "Jan Pietersen" een instantie van het informatieobjecttype "(natuurlijk) persoon". In ons voorbeeld van (het informatieobject:) "de door beambte Janssen op 1 september 2021 vastgelegde verklaring van een aangever" kan er een informatieobjecttype zijn gedefinieerd met de naam "Procesverbaal Aangifte" die beschrijft welke gegevens in een aangifte opgenomen kunnen worden.

Het informatieobjecttype kan ook de receptuur (via afleidingsregels) omvatten aan de hand waarvan elementen van een informatieobject van dat type geconstrueerd worden.

5.2.3 Informatieobjectrepresentatie

Als we spreken over een informatieobject, dan spreken we alleen over de informatie-inhoud. Die informatie-inhoud, en dus het informatieobject, heeft betekenis en bestaat ongeacht de vorm waarin die informatie-inhoud wordt

uitgedrukt. Een informatieobject kan echter alleen verwerkt worden als het informatieobject uitgedrukt is in een bepaalde vorm die waargenomen en begrepen kan worden door mensen of machines. De vorm met inhoud waarin een informatieobject wordt uitgedrukt wordt aangeduid met *informatieobjectrepresentatie*.

Definitie Informatieobjectrepresentatie
De uitdrukking van de informatie-inhoud van een informatieobject in een voor mensen of machines waarneembare vorm.

Iedere representatie van een informatieobject kent ook een eigen identiteit. Daardoor kan ook naar iedere informatieobjectrepresentatie eenduidig worden verwezen door gebruik van het identificatiekenmerk ervan. Van iedere informatieobjectrepresentatie moet natuurlijk ook duidelijk zijn van welk (uniek aanwijsbaar) informatieobject deze een uitdrukking is.

5.2.4 Informatieobjecttype-representatietype

De vormen waarin een informatieobject wordt uitgedrukt, kunnen veelal niet vrijelijk worden gekozen. Om doelmatig en efficiënt te kunnen samenwerken in de SRK, worden standaarden bepaald voor de vormen waarin informatieobjecten verwerkt mogen worden. Zo'n vorm-standaard noemen we een representatietype. Van ieder informatieobjecttype moet vervolgens worden bepaald welke van de standaard representatietypen[34] zinvol en toegestaan zijn om een informatieobject van dat type in uit te drukken. Bij de beschrijving van een informatieobjecttype hoort dan ook aangegeven te worden wat de toegestane representatietypen voor dat informatieobjecttype zijn. Dat duiden we aan met de term informatieobjecttype-representatietype. In ons voorbeeld is dat "Procesverbaal Aangifte als een pdf in een specifieke opmaak, zoals voorgeschreven door het bijbehorende representatietype".

Definitie Informatieobjecttype-representatietype.
Een representatietype waarin een informatieobject van een bepaald informatieobjecttype kan worden uitgedrukt.

5.2.5 Exemplaar

Tenslotte kan het zijn dat van dezelfde informatieobjectrepresentatie twee precies dezelfde exemplaren bestaan. Zo kunnen van pdf 9 van PV aangifte Janssen op 1 september 2021, aangeduid met *PVA-123/pdf-9*, twee exemplaren bestaan, namelijk *PVA-123/pdf-9/ex-1* [35]in de systemen van de politie, en *PVA-123/pdf-9/ex-2* bij het OM, die verder op geen enkele wijze onderscheidbaar zijn, noch in inhoud, noch in representatie, noch in enig ander kenmerk (b.v. digitaal waarmerk) – en dat van elkaar kunnen onderscheiden van die exemplaren is op ketenniveau ook helemaal niet relevant. Desgewenst kunnen we zeggen (als we bij ketenpartners binnenshuis zouden kunnen kijken):

PVA-123/pdf-9/ex-2 *bevindt-zich-op-locatie* OM

Kenmerkend voor een exemplaar is dat die fysiek is, en in tijd en ruimte uniek; één exemplaar kan (in ieder geval volgens klassieke mechanica) op hetzelfde moment maar op één plaats zijn. Daarnaast kunnen aan één exemplaar bepaalde waarborgen verbonden zijn, zoals een natte handtekening (op een papieren exemplaar) of een digitaal waarmerk (van een pdf) of een daarover vastgelegde hash-waarde (van een record in een database).

5.3 Traceerbaarheid van objecten

Als partijen in de strafrechtketen informatie uitwisselen, dan ontstaan daarbij exemplaren van dezelfde informatieobjectrepresentatie bij verschillende partijen. Om goed af te kunnen spreken wie nu welke informatieobjecten aan wie beschikbaar stelt beschrijven we die als informatiediensten.

Definitie Informatiedienst.
Een informatiedienst is een dienst die informatieobjecten vastlegt, deelt of afleidt. Het gaat hierbij om het leveren van (exemplaren van) specifieke informatieobjecten (van één informatieobjecttype in bepaalde representatietypen).

Net zoals voor ieder ander soort dienst geldt ook hier dat het leveren ervan geschiedt op basis van afspraken tussen leverancier en afnemer(s), uitgedrukt in onder meer een dienstovereenkomst en leverings- en aansluitvoorwaarden. In het bijzonder geldt dat de informatieobjecten worden geleverd voor een afgesproken doel (doelbinding) en op basis van een grondslag.

Bij iedere informatie-uitwisseling conform de Interactiepatronen is sprake van een informatiedienst. Zo is het leveren van een attendering een informatiedienst, evenals het leveren van een informatieproduct bij vraaggestuurde informatiedeling. Maar ook ook het verzoek

[34] Papier, document (word, pdf, etc.), XML-bericht, gesproken, beeld, etc.

[35] Merk op dat de hier gegeven exemplaarIDs (*ex-1*, *ex-2*) alleen bedoeld zijn om ze in deze toelichtingen te kunnen onderscheiden. Geenszins is hier bedoeld iets te zeggen over naamgevings-conventies van exemplaren. Zo zou in bepaalde wijzen van digitaal waarmerken het geven van een andere bestandsnaam al tot een ander digitaal waarmerk kunnen leiden, wat dit dus niet alleen tot een ander exemplaar, maar zelfs tot een andere representatie zou maken.

om een bedrijfsdienst volgens het afsprakenpatroon heeft een informatie-inhoud, en het zenden van dat verzoek is ook een informatiedienst.

Aangezien informatieobjecten alleen kunnen bestaan in een specifieke representatie zal de afspraak over die informatiedienst dus ook iets zeggen over in welke representatie dat informatieobject dan beschikbaar komt.

Op deze wijze ontstaan meerdere exemplaren van informatieobjecten in soms verschillende representatievormen bij diverse partners.

In ons voorbeeld kan bijvoorbeeld de politie toezeggen aan het openbaar ministerie dat zij van Procesverbalen Aangifte die nodig zijn in de vervolgingsfase een exemplaar kunnen verkrijgen in PDF/A-formaat of in een specifieke op XML gebaseerde representatievorm.

Conform het mantra van de KDA willen we '[…] gegevens over personen, zaken, beslissingen en bewijsmiddelen uitwisselen […] zodanig dat gegevens samenhangend beschikbaar zijn vanuit de verschillende perspectieven […]'.

Een eerste vereiste daarbij is dat van de verschillende exemplaren van representaties van informatieobjecten die in de keten bestaan duidelijk is of het nog steeds hetzelfde informatieobject betreft. Dit is nodig omdat met name in het strafrecht de integriteit en authenticiteit van het informatieobject voldoende aantoonbaar moet zijn om de informatie-inhoud te kunnen gebruiken binnen de juridische context van het strafrecht.

Hiervoor is een basisafspraak nodig dat exemplaren van informatieobjecten niet gewijzigd worden na initiële vastlegging van het eerste exemplaar. Ieder exemplaar dat daarna ontstaat moet aantoonbaar 'gelijk' zijn aan het initiële exemplaar. Het 'gelijk' zijn van twee exemplaren betreft het vooraleerst de informatie-inhoud, dus het informatieobject zelf. In sommige juridische situaties speelt echter ook de representatievorm een rol en moet ook die 'gelijk' zijn.

Een exemplaar van een representatie van een informatieobject kent dus altijd drie identiteiten. De eerste identiteit betreft de informatie-inhoud, het informatieobject. De tweede identiteit betreft het informatieobject in een specifieke representatievorm. De derde identiteit betreft die van het exemplaar van een informatieobjectrepresentatie. In ons voorbeeld is de informatie-inhoud geïdentificeerd door een administratief afgegeven uniek nummer van de aangifte (bijvoorbeeld BVH-nr) of door een combinatie van identificerende gegevens (bijvoorbeeld de verantwoordelijke opsporingsambtenaar en de datum, tijd en locatie van ondertekening). De tweede identiteit is een uitbreiding van de eerste, aangevuld met de unieke representatie. De derde identiteit vult de eerste twee aan met die van het unieke exemplaar.

Informatieobjecten zijn vaak samengesteld uit andere informatieobjecten, ieder met een eigen identiteit. In ons voorbeeld zou dat de gegevens van de aangever kunnen zijn. Door deze apart van een identiteit te voorzien ontstaat de mogelijkheid om gegevens aan elkaar te relateren. Bijvoorbeeld om te weten of de aangever nog andere aangiftes gedaan heeft.

5.4 Relateren van objecten

Objecten hebben onderlinge relaties, en dat wordt weerspiegeld in de relatie tussen de bijbehorende *informatie-objecten*. Zo is justitiabele Piet *verdachte-in* zaak A, en *veroordeelde-in* zaak B. En natuurlijk persoon Fatima is *getuige-in* zaak A, en *slachtoffer-in* zaak B. Die relaties kunnen worden uitgedrukt als relaties tussen informatieobjecttypen, zoals "JUSTITIABELE *is-verdachte-in* ZAAK".

5.5 Traceerbaarheid van exemplaren

Zoals gezegd is het van wezenlijk belang dat, als partners exemplaren van informatieobjecten uitwisselen, er zekerheid gekregen kan worden in hoeverre dat informatieobject nog steeds "hetzelfde" is. In veel gevallen bepaalt dat de juridische geldigheid van een bepaald exemplaar van een informatieobject-representatie. Dit vereist dat partners afspraken maken over onder welke voorwaarden de juridische geldigheid [36]in stand blijft als een nieuw exemplaar wordt ontvangen van een informatiedienst.

Hierbij helpt het om in de afspraken tussen partners expliciet te zijn over de vier varianten volgens welke een nieuw (exemplaar van een) informatieobject kan worden gemaakt.

levert / variant	(inhoud/semantiek) informatieobject	(syntax) representatie	(medium) exemplaar
kopiëren	zelfde	zelfde	ander
her-representeren	zelfde	ander	ander
extraheren	ander, gedeeltelijk zelfde juridisch effect	ander	ander
bekrachtigen	ander – maar 100% zelfde juridisch effect	ander	ander

[36] Zoals in 3.2 beschreven zijn voor het voldoen aan de BIVA-eisen organisatorische, procesmatige en IV/ICT technische maatregelen nodig. Een authentiek en integer document in onbevoegde handen geeft in die handeling nog geen rechtsgeldigheid.

5.5.1 Variant 1 – kopiëren

Samengevat: met kopiëren bedoelen we dat het verkregen informatieobject exact dezelfde informatie-inhoud en exact dezelfde representatie heeft als het informatieobject waarvan het afgeleid is; het is alleen een ander exemplaar. De juridische geldigheid is dus eveneens exact gelijk.

Kopiëren neemt dus als input een zeker exemplaar van een informatieobjectrepresentatie (dus met een zekere inhoud, in een zekere vorm en met bepaalde waarborgen) en levert als output een nieuw exemplaar met dezelfde informatie-inhoud in dezelfde informatieobjectrepresentatie, inclusief alle waarborgen (integriteit, authenticiteit, zelfde ID van inhoud en ID van representatie; ander ID van exemplaar). PVA-123/pdf-9/ex-2 *bevindt-zich-op-locatie* OM

Voortbouwend op het voorbeeld onder5.2.5 Exemplaar: stel kopiëren neemt als input het digitaal gewaarmerkte exemplaar 1 van pdf 9 van Proces Verbaal Aangifte 123, aangeduid met *PVA-123/pdf-9/ex-1* en produceert als output het (eveneens digitaal gewaarmerkte) exemplaar *PVA-123/pdf-9/ex-2*. Desgewenst kunnen de digitale waarmerken van deze twee exemplaren worden vergeleken, zodat zekerheid wordt verkregen over hun onderlinge "gelijkheid".

Het resultaat van kopiëren noemen we een kopie. Een "kopie" is per definitie "juridisch equivalent" met het "origineel" – even los van het feit dat de bruikbaarheid van die begrippen in de digitale wereld laag is (zie hoofdstukken 2 en 3. Desgewenst kunnen we beweringen doen, en ter wille van traceerbaarheid vastleggen, zoals

PVA-123/pdf-9/ex-2 *is-kopie-van* PVA-123/pdf-9/ex-1

en

PVA-123/pdf-9/ex-2 *is-juridisch-equivalent-aan* PVA-123/pdf-9/ex-1

5.5.2 Variant 2 – herrepresenteren

Bij herrepresenteren ontstaat een nieuwe representatie van hetzelfde informatieobject. De informatie-inhoud blijft dus exact hetzelfde, wel ontstaat een nieuwe representatie-ID (en natuurlijk ook een exemplaar-ID).

Voorbeelden hiervan zijn:

- papier naar pdf of andersom;
- pdf 1.7 naar pdf/A;
- multimedia-conversies, zoals het omzetten van wav naar mp3 of van wmv naar mp4;
- xml naar json of andersom;
- xml naar pdf;
- transcriptie van audio.

Zeker bij de huidige stand van de techniek rijst de vraag in hoeverre bij de aangegeven voorbeelden de informatie-inhoud echt 100% hetzelfde blijft (immers, dan mag het geen herrepresentatie heten). Bij het antwoord kijken we naar 2 aspecten: relevantie en correctheid. Dit zal ook de juridische geldigheid / equivalentie van de nieuw gecreëerde representatie bepalen.

Zo is redelijk duidelijk dat bij een omzetting tussen specifieke technische versies van pdf (zoals 1.7 naar pdf/A) de relevante inhoud geheel hetzelfde is en we een hoog vertrouwen hebben in de technische correctheid van deze omzetting. Zo ook voor diverse multimediaconversies en gestructureerde berichten.

Bij automatische transcriptie van een audiobestand vallen bijvoorbeeld de toonhoogte en spreekpauzes van de rechter weg – en dat is verlies aan informatie-inhoud. Tegelijk wordt diens uitgesproken tekst niet geïnterpreteerd, dus beschouwen we de relevante informatie-inhoud als dezelfde. Op het aspect van correctheid zal getoetst moeten worden in hoeverre deze automatische transcriptie-technologie al voldoende foutloos werkt.

5.5.3 Variant 3 – extraheren

Bij extraheren ontstaat een nieuw informatieobject (met een eigen ID) door filtering van het oorspronkelijke informatieobject – bepaalde gegevens worden weggelaten, bijvoorbeeld uit oogpunt van privacy, "need-to-know", dataminimalisatie, of gewoon efficiency. Enkele hiervan zijn:

- van een proces-verbaal van aangifte wordt een geanonimiseerd extract aan de advocaat van de verdachte verstrekt; deze kan "juridisch equivalent" worden verklaard;
- van een bewakingsfilmpje van een winkelcentrum van 6 uur zijn de 2 minuten geselecteerd vanaf welke voor het eerst de verdachte in beeld kwam;
- aan AICE wordt een vonnis-extract verstrekt dat voldoende is om alle sanctiecomponenten te bepalen.

Sommige extracten kunnen "juridisch equivalent" (voor een bepaald doel) worden verklaard. Bijvoorbeeld dat de geanonimiseerde versie van het proces-verbaal van aangifte mogelijk voldoet aan equality-of-arms in de rechtbank.

5.5.4 Variant 4 – bekrachtigen

Bij bekrachtigen ontstaat een nieuw informatieobject (met een eigen ID) door aan een ander informatieobject een persoonsgebonden waarmerk van een beëdigde toe te voegen, waarmee een juridische waardering wordt toegekend. Een voorbeeld hiervan is het voorzien van een apostille: "Een apostille is een stempel of sticker van de rechtbank op een officieel document, die aantoont dat de handtekening op het document echt is".

Soms dient eerst een kopie, herrepresentatie of extract te worden gemaakt, alvorens deze bekrachtigd kan worden. Denk hierbij aan een gewaarmerkt vonnis, die tot stand komt door een vonnis (in pdf) af te drukken, te bekrachtigen en opnieuw te scannen.

In specifieke gevallen wordt een geprotocolleerde omzetting toegepast. Het meest bekende voorbeeld hiervan is "scannen onder substitutie". Dit is een combinatie van een geprotocolleerde herrepresentatie (scannen van papier naar pdf) én de bekrachtiging dat deze omzetting voldoet aan de afgesproken kwaliteitscriteria, waardoor het resultaat als "juridisch equivalent" wordt beschouwd en het papieren origineel zelfs niet meer nodig is.

5.5.5 Traceerbaarheid

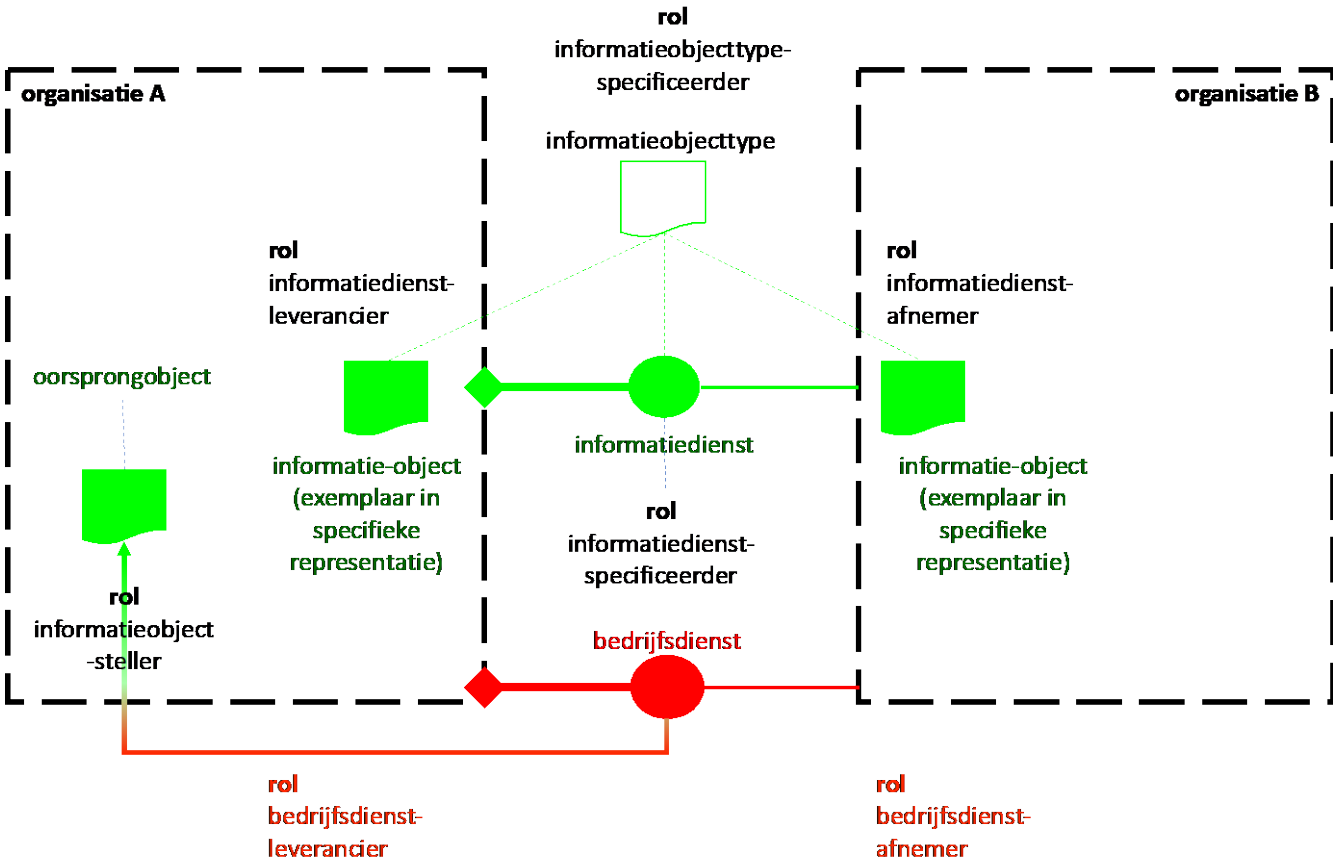
Bij traceerbaarheid van informatie-objecten gaat het erom te weten hoe een informatieobject tot stand is gekomen. Door de gebruikte variant én de relaties met de als input gebruikte informatieobjecten bij te houden wordt de zogenaamde bewaarketen en bewerkingsketen van informatie-objecten transparant. Hiermee kan desgewenst de juridische geldigheid van uitgewisselde gegevens vastgesteld worden.

NB1 Deze beschrijving van varianten dient, mede aan de hand van praktijkcasussen, nog nader getoetst te worden op juridische aannames en uitgangspunten. Zijn bijvoorbeeld begrippen "juridische equivalent" of "juridisch vergelijkbaar" goed toegepast?

NB2 Deze beschrijving van varianten dient op MECE getoetst te worden. Waar laat je bijvoorbeeld het omzetten van een mp3-vonnis naar een xml-bericht – immers, de toonzetting verdwijnt (extractie?), en structuur wordt toegevoegd.

5.6 Verantwoordelijkheden tussen ketenpartijen

Op basis van de in het voorgaande geïntroduceerde bouwstenen voor informatieverwerking kunnen nu ook duidelijke afspraken gemaakt worden over de verschillende informatieverantwoordelijkheden tussen ketenpartijen. Op enkele rollen daarbij gaan we nu nader in, zoals aangegeven in Figuur 8.



Figuur 8 Informatieobjecten, informatiediensten en rollen

5.6.1 Rondom informatiedienst

Een informatiedienstleverancier levert exemplaren van de afgesproken informatieobjecttypen in afgesproken representatietypen, volgens de leveringsovereenkomst en de leveringsvoorwaarden, en zolang de informatiedienstafnemer aan de aansluitvoorwaarden voldoet. Daarbij toetst de informatiedienstleverancier of de gevraagde informatieobjecten passen bij de grondslag en doelbinding van de informatiedienstafnemer.

Een informatiedienstafnemer kan exemplaren van afgesproken informatieobjecttypen in afgesproken representatietypen ontvangen, volgens de leveringsovereenkomst en de leveringsvoorwaarden, zolang die informatiedienstafnemer aan de aansluitvoorwaarden voldoet. Daarbij reikt de informatiedienstafnemer alles aan wat nodig is voor toetsing op grondslag en doelbinding door de informatiedienstleverancier

Gegeven een te leveren informatieobjecttype ontwerpt de Informatiedienstspecificeerder de te leveren informatiedienst, inclusief de leverings- en aansluitvoorwaarden. In de strafrechtketen wordt deze rol ingevuld door een collectief van partijen die in samenspraak specificeren, waarbij uiteindelijk één partij de beslisser/verantwoordelijke is.

Voorbeelden van leveringsvoorwaarden zijn: de betrouwbaarheidsniveau (a la STORK/eIDAS) van identificatie en autorisatie van de afnemer, Quality of Service, procedure voor het melden van leveringsgebreken, etc.

Voorbeelden van aansluitvoorwaarden zijn: het meewerken aan audits en het actief aan kunnen tonen dat aan aansluitvoorwaarden is voldaan – zoals door te blijven participeren in ketentesten (inclusief het kunnen oplossen van foutherstel binnen een afgesproken termijn (MTBR)).

5.6.2 Rondom informatieobject

Een informatieobjecttypespecificeerder specificeert het informatieobjecttype van informatieobjecten. In de strafrechtketen wordt deze rol ingevuld door een collectief van partijen die in samenspraak specificeren, waarbij uiteindelijk één partij de beslisser/verantwoordelijke is.

Dit specificeren omvat als eerste de informatie-inhoud, zoals welke gegevens het (maximaal) bevat, in welke syntax die wordt uitgedrukt en welke afleidingsregels daarbij eventueel worden gebruikt. Daarnaast omvat het de mogelijke representaties van het informatieobject, zoals pdf, xml of papier – dus de specificaties van informatieobjecttyperepresentatietypen. Tenslotte omvat het de beoogde kwaliteiten van dat informatieobject zelf (zoals hoe Juist / Actueel / Nauwkeurig / Compleet (JANC) de gegevens daaruit moeten zijn; zie ook [RGK] en het NORA-raamwerk gegevenskwaliteit (in wording)).

Een informatieobjectsteller formuleert, als direct gevolg van de uitvoering van een bedrijfsdienst, voor het eerst een informatieobject in een bepaalde representatie, en is dus als enige daarvoor inhoudelijk verantwoordelijk. Het informatieobject dat dan ontstaat noemen we ook wel oorsprongobject. De rol van informatieobjectsteller zou door een politierechter zelf kunnen worden ingevuld, wiens mondelinge rechterlijke uitspraak als geluidsbestand wordt vastgelegd. Of een meervoudige strafkamer, wier vonnis schriftelijk wordt vastgelegd.

Definitie oorsprongobject
Een oorsprongobject is een informatieobject dat ontstaan is naar aanleiding van een oorspronkelijke actie (zoals beslissen, beoordelen, vervoeren, insluiten) door de ketenpartij die ook verantwoordelijk is voor die oorspronkelijke actie.

6. Ketencommunicatievoorzieningen conceptueel

In gesprekken over de ketencommunicatievoorzieningen (KCV) blijkt dat er verschillende beelden zijn over wat deze voorzieningen behelzen. De beelden lopen uiteen van zoemende gezamenlijke IT waar je "een stekker in steekt", tot alleen maar afspraken en standaarden: "alleen maar papier". De waarheid ligt, volgens de traditie, in het midden.

In dit hoofdstuk geven we een verdere uitleg van de ketencommunicatievoorzieningen en het onderscheid met ketensteunpuntvoorzieningen. De eerste 4 paragrafen zijn eerder beschreven in het "positionpaper Ketencommunicatievoorzieningen" [PKCV]. Aangeboden en vastgesteld door het OGB maart 2021.

Eerst gaan we in op de aanleiding en het concept. Daarna ordenen we de 11 ketencommunicatievoorzieningen in samenhangende clusters. In de paragraaf ICT-perspectief geven we een indicatie wat strafrechtketen-specifiek is, waar een gezamenlijkheid in ICT mogelijk is.

Wellicht ten overvloede: de ketencommunicatievoorzieningen gaan over de interoperabiliteit op de semantische en technische lagen van het EIF-Raamwerk.

6.1 Achtergrond

De leidende principes van het Opdrachtgeversberaad (OGB) en het Bestuurlijk Ketenberaad (BKB) en de Ketendoelarchitectuur (KDA) gaan uit van de rechtsstatelijke verantwoordelijkheden en het losjes koppelen ('loosely coupled') van ieders informatievoorziening.

Tegelijkertijd maken wederzijdse afhankelijkheden in de digitalisering van de strafrechtketen communicatie en afspraken daarover nodig. Het sleutelwoord hierbij is interoperabiliteit. Hieronder verstaan we het verhogen van de capaciteit van organisaties om te kunnen samenwerken ondersteund door beheersbare en aanpasbare informatievoorzieningen (ICT).

Vertaald naar de KDA: zorgen voor gestandaardiseerde taal en techniek, de lagen 3 en 4 van het EIF-Raamwerk. Dit vergroot het aanpassingsvermogen en dat vereenvoudigt de implementatie van wetswijzigingen en het aansluiten van nieuwe ketenpartners.

6.2 Het concept

De Ketencommunicatievoorzieningen vormen een raamwerk van elf samenhangende 'onderwerpen'. Het is het leidingstelsel, de energie en water voor de samenwerking op informatievoorziening in de keten. Zij vormen daarmee de basis voor onder andere de zekerheid dat een dossier compleet is, dat de verstrekte stukken daadwerkelijk ontvangen zijn, dat de inhoud van informatie ongewijzigd is en de authenticiteit daarvan is vast te stellen. Zie voor verdere onderbouwing het rapport "Toekomst van de strafrechtspleging" van de Commissie van de Emster" [TRSP] en de KDA.

Ketencommunicatievoorzieningen zijn onderwerpen waar ketenpartners met elkaar:

- afspraken over moeten maken;
- zo nodig standaarden voor moeten afspreken en toepassen;
- waarvoor eigen ICT-voorzieningen veelal aangepast of ontwikkeld moeten worden;
- waarvoor eventueel een gezamenlijke ICT-voorziening nodig is;
- toezicht en handhaving moeten inrichten.

De afspraken[37] gaan over zaken als: waarover communiceren ketenpartners, met welk doel en op basis van welke grondslag en waar komt de informatie vandaan (wat is de bron), welke technische afspraken maken we, hoe geven we invulling aan compliance-eisen.

De standaarden moeten zorgen dat per situatie bestaande oplossingen toegepast worden. En dat investeringen in gegevensuitwisseling tussen alle ketenpartners werken en niet slechts tussen twee. Voorbeelden hiervan zijn JenV referentiegegevens, strafrechtketen multimedia-standaarden, de Rijksstandaard Digikoppeling en de Justitie berichtenstandaard EBV.

Vervolgens zullen deze afspraken en standaarden in ICT geïmplementeerd moeten worden. Dit vraagt aanpassingen binnen de eigen informatievoorziening van ketenorganisaties en in specifieke gevallen vraagt het ook om SRK- of JenV-brede ICT-voorzieningen.

Dit hele samenstel van komen tot en onderhouden van afspraken en standaarden, het toezicht daarop, de eigen ICT en eventueel een gezamenlijke voorziening omvat een ketencommunicatievoorziening. De toepassing van deze ketencommunicatievoorziening wordt begrensd tot dat wat voor de strafrechtketen nodig is.

Figuur 9 Ketenvoorzieningen: afspraken, standaarden en ICT

[37] Omdat veel ketenpartners in meerdere ketens opereren wordt waar mogelijk aangesloten bij Rijks- en JenV-afspraken en standaarden.

Een voorbeeld: E-Handtekening.

Om de integriteit en authenticiteit van een uitgewisseld digitaal document (pdf, filmpje, bericht, dossier, etc.) zeker te stellen spreken de ketenpartners af dat zo'n document digitaal getekend en gewaarmerkt dient te zijn. En dat ontvangers op één plaats kunnen controleren dat een document niet is gecorrumpeerd. De eerste set afspraken.

Afspraken:
Dit vraagt nadere afspraken over het zetten van een digitale handtekening en waarmerken. Vereenvoudigd: de condities waaronder een digitale handtekening houdbaar is en hoe hierop toe te zien (BIVA eisen). O.a. het zeker stellen dat een document digitaal getekend is door de bevoegde persoon en niet door een voorbijganger. En het vaststellen wat de geldigheidsperiode van een digitale handtekening is (5 jaar, levenslang?).

Standaarden:
Voor de digitale handtekening en het waarmerken zijn ook technische standaarden nodig: het algoritme voor de handtekening, de wijze van valideren en tijdige vernieuwing van het algoritme voordat het gekraakt wordt.

Ketenpartner ICT
De uitwerking is bekend: De afspraken zijn gemaakt inclusief periodieke audits hierop. De digitale handtekening wordt gezet met verschillende software in eigendom van de verschillende ketenpartners of van een gezamenlijke toepassing. Zo gebruikt de Rechtspraak ook de oplossing van het OM. De software voor de handtekening zetten voldoet aan het JenV-breed afgesproken algoritme.

Gezamenlijke ICT
De validatie wordt ondersteund met een ICT-voorziening met JenV reikwijdte (GAAV) met bijbehorende verantwoordelijkheden, governance en financiering.

6.3 Samenhang

Als we digitaal willen communiceren in de keten dienen we op ketenniveau vier vragen te beantwoorden:

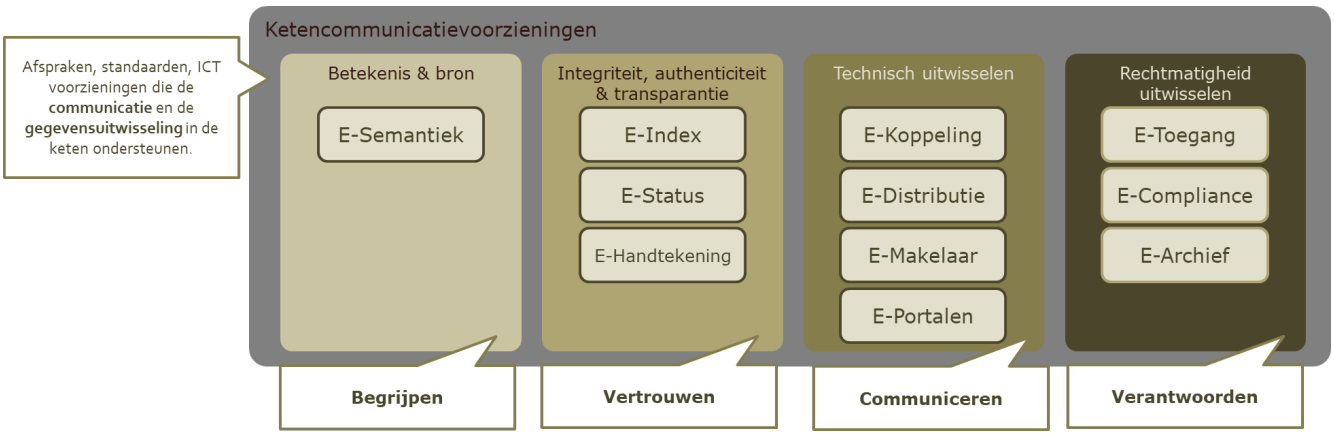
1) Allereerst moeten we weten waar we over communiceren, met welk doel en waar de informatie vandaan komt.
2) Vervolgens is de vraag: hoe kan ik de (het) verkregen informatie(object) vertrouwen?
3) Dan is de vraag: hoe komen informatieobjecten van de ene ketenpartner bij de andere?
4) Hoe tonen we aan dat we voldoen aan wet- en regelgeving?

Langs deze indeling zijn ook de ketencommunicatievoorzieningen te ordenen:

1) Voorziening gericht op de **betekenis** van data, **bronnen**: "Wat betekent dit? En hoe noemen we dit?" en "Waar is welke data voor wie te verkrijgen?". Dit is het gebied van E-Semantiek;
2) Voorzieningen gericht op **integriteit en authenticiteit** van data en **transparantie**: de basis onder de bewaarketen en de bewerkingsketen. Dit omvat E-Status, E-Index en E-Handtekening;
3) Voorzieningen gericht op techniek voor het **uitwisselen** van data. Dit omvat E-Koppeling, E-Distributie, E-Portalen en E-Makelaar;
4) Voorzieningen gericht op het **voldoen** aan wet- en regelgeving. Als we data uitwisselen dienen wij aan wetgeving te voldoen. Dit omvat E-Compliance, E-Archief en E-Toegang.

Uiteraard zijn er relaties tussen deze vier werkingsgebieden. De onderlinge afhankelijkheden werken we uit in hoofdstuk "7".

Deze ordening is ook een goede basis voor het organiseren van overleggen in de keten. Dit helpt om de juiste betrokkenen te selecteren om mee te praten. En het geeft samenhang, zowel in inhoud als in benodigde expertise.



Figuur 10 Clustering ketencommunicatievoorzieningen

6.4 ICT-perspectief

Het voorbeeld van E-Handtekening maakt duidelijk dat afspraken altijd en standaarden bijna altijd van toepassing zijn. Alsook dat er vrijwel altijd sprake is van een vertaling in ICT. Immers alle digitaal uitgewisselde informatie (m.b.v. E-Koppeling en E-Distributie) dient te voldoen aan de afgesproken taal van de keten (E-Semantiek). Een digitale handtekening kan niet zonder ICT.

Daarmee is niet gezegd dat dit gezamenlijke ICT is. Zoals het voorbeeld duidelijk maakt kan het ICT bij de ketenpartners zijn alsook (voor een deel) gezamenlijke ICT.

De SRK-AR gaat ervan uit dat voor een deel van de ketencommunicatievoorzieningen aanpassing van gemeenschappelijke ICT (JenV reikwijdte) nodig is. Het gaat dan om de eerdergenoemde E-Handtekening (GAAV), en bestaande voorzieningen voor E-Toegang (IAM), E-Archief (CDD) en E-Distributie (Jubes/API-strategie).

Een groot deel van de ICT van ketenvoorzieningen ligt echter bij ketenpartners. Gestandaardiseerde ontsluiting van de informatie (E-Koppeling op basis van E-Semantiek) zal een forse inspanning vragen. Ook toegang, gegevensbescherming en archivering (E-Toegang, E-Compliance en E-Archivering) kennen vooral ICT achter de voordeur van de ketenpartner.

Om losjes te koppelen en de verschillen in taal en techniek (tijdelijk) te overbruggen binnen en buiten de keten voorziet de SRK-AR gezamenlijke (SRK reikwijdte) ontwikkeling van E-Distributie (strafrechtketen specifiek) en E-Makelaar.
In de praktijk zullen Ketenpartners op verschillende momenten in tijd aan (delen van) de afspraken en standaarden (E-Koppeling en E-Semantiek) gaan voldoen. We moeten zorgen dat bij nieuwe of vervangende informatie-uitwisseling minimaal aan één kant aan de nieuwe afspraken wordt voldaan. E-Distributie kan worden ingezet als de andere partner nog niet aan de afspraak kan voldoen. Daarmee wordt voorkomen dat beide op de oude voet verder gaan. Dit met inachtneming van de uitgangspunten beschreven in 4.8 "IV organiseren in de keten".

Voor het traceerbaar maken van afspraken en informatie en de samenhang daartussen zijn E-Status en E-Index voorzien. Dit is nieuw voor de keten en zal zich grotendeels vertalen in ICT bij de ketenpartners en voor een deel in gezamenlijke ICT. Om de gegevens uit E-Status en E-Index te kunnen gebruiken voor een bewaar- en/of een bewerkingsketen is minimaal een gezamenlijk ontwerp van E-Status en E-Index nodig. Alsook de realisatie van gezamenlijke onderdelen. Deze gezamenlijke aanpak draagt tevens bij aan het delen van schaarse kennis en voorkomt dat het wiel meerdere malen wordt uitgevonden.

Een kort woord over E-Semantiek, de hoeksteen van de semantische/informationele interoperabiliteit. Om te komen tot eenheid van taal en bronnen is één plaats in de keten nodig om deze afspraken vast te leggen en te ontsluiten. Dat vraagt een fors rijkere ICT-voorziening en ondersteuning dan nu beschikbaar voor de keten.

Voorgaande laat zich samenvatten in onderstaande tabel

	Afspraken	Standaarden	Impact op en Eigen ICT	SRK ICT	JenV ICT
E-Semantiek	X	X	X	X	
E-Index	X	X	X	X	
E-Status	X	X	X	X	
E-Handtekening	X	X	X		X
E-Koppeling	X	X	X		
E-Distributie	X	X	X	X	X
E-Makelaar	X	X	X	X	
E-Portalen	X	X	X	?	
E-Compliance	X	X	X		
E-Toegang	X	X	X		X
E-Archief	X	X	X		X

6.5 Onderscheid steunpuntvoorzieningen

Omdat het onderscheid tussen ketensteunpuntvoorzieningen (KSV) en ketencommunicatievoorzieningen (KCV) soms niet helder is geven we een korte duiding van het verschil. Beide ondersteunen de samenwerking in de keten, zij het op verschillende architectuurlagen.
Ketensteunpuntvoorzieningen bevinden zich op de proces- en organisatie-laag.

Er zijn processen waarbij gezamenlijk opgetrokken moet worden. Denk aan verifiëren van identiteiten (biometrie en SKDB), slachtoffers informeren (KBSP), beheer beslag goederen en forensisch materiaal, zittingsplanning en foutherstel.

Een ketensteunpuntvoorziening vraagt dus afstemming van de afzonderlijke bedrijfsprocessen waarbij een gezamenlijkheid ontstaat en tegelijkertijd iedere ketenpartner verantwoordelijk blijft voor de eigen processen en gegevens. De gezamenlijkheid beperkt zich tot datgene wat iedere ketenpartner nodig heeft om haar primaire proces uit te voeren.

Ketensteunpuntvoorzieningen zijn een nuancering op het leidende principe "geen gezamenlijke primaire procesapplicaties op ketenniveau".

Het leidende principe van het OGB en BKB roept op die gezamenlijkheid zo beperkt mogelijk te houden en tegelijk zeer duidelijk te zijn over verantwoordelijkheden en besturing. Keuze voor een ketensteunpunt vraagt daarom expliciete besluitvorming van het OGB.

7. Ketencommunicatievoorzieningen uitwerking

In hoofdstuk 6 is het concept van de ketencommunicatievoorzieningen beschreven. Ook zijn de elf KCV'en geordend in vier gebieden. In deze volgorde worden de KCV'en behandeld.

1) *Betekenissen en bronnen:*
    - *E-Semantiek*
2) *Integriteit, traceerbaarheid en transparantie:*
    - *E-Index*
    - *E-Status*
    - *E-Handtekening*
3) *Technisch uitwisselen:*
    - *E-Koppeling*
    - *E-Distributie*
    - *E-Makelaar*
    - *E-Portalen*
4) *Rechtmatigheid uitwisselen:*
    - *E-Compliance*
    - *E-Toegang*
    - *E-Archief.*

In de KDA 1.0 is wel het interactiepatroon "Notificeren", nu "Attendering", beschreven. Er is echter geen uitwerking gemaakt naar een ketencommunicatievoorziening. In de verdieping positioneert de SRK-AR de ondersteuning van dit patroon bij de E-Makelaar.

Het hoofdstuk sluit af met een waarschuwing om terughoudend te zijn en bewust af te wegen welke relaties tussen KCV'en geautomatiseerd ondersteund kunnen worden. Zowel tijdens het ontwerp als het gebruik.

7.1 Betekenissen en bronnen

7.1.1 E-Semantiek

E-Semantiek betreft het informationele kennisdomein, de bibliotheek van begrippen, definities en bronnen van en voor de keten. Zonder afgesproken begrippen, verantwoordelijkheden en bronnen voor informatieobjecten is communicatie niet mogelijk.

☞ Alle afspraken over betekenissen, bronnen, nummerstelsels, afleidingsregels, grondslagen, doelen, processen en diensten zijn op één plaats[38], de te ontwikkelen SRK-Repository te vinden.

De SRK-Repository, met alle bijbehorende processen is de kern van E-Semantiek. De reikwijdte omvat meer dan de primaire associatie met Canoniek DataModel Strafrechtketen (CDM).

Onder het bereik van E-Semantiek valt:

1) Het (laten) onderhouden en publiceren van (typeniveau) onderstaande, altijd inclusief degene (ketenpartner / tafel) die het heeft vastgesteld, en dus verantwoordelijk is:
- SRK Thesaurus;
- Actorrollen;
- Processen, bedrijfs- en informatiediensten onderling gerelateerd en gerelateerd aan actorrollen en verantwoordelijkheden, grondslagen en doelbinding
    - Producten- en dienstencatalogi;
- Gegevensmodellen (op verschillende lagen) met daarin opgenomen:
    - Nummerstelsels en wijze van uniciteit;
    - Afleidingsregels;
    - Referentiegegevens[39];
    - Stamdata.
- Informatieproducttypen inclusief verantwoordelijkheden, doelbinding en grondslagen, gerelateerd aan bedrijfs- en informatiediensten.
    - Attenderingen, afspraken vallen hier ook onder.
- (Archief) Metadatastandaarden;
- Afleidingsregels voor communicatie met andere partijen buiten de strafrechtketen (zoals Migratieketen, Zorgketen en Burgerdomein). Inclusief de verantwoordelijke voor de afleidingsregel. Omvat omzetting van coderingsregels, syntax en labels;
- Gegevenswoordenboeken;
- Berichtenboeken gekoppeld aan processen en informatiediensten;
- Standaarden voor modellering en vastlegging van bovenstaande in E-Semantiek;
- Begrippenlijst.

Van ieder hierboven beschreven type in E-Semantiek dient bekend te zijn: wie is verantwoordelijk voor de inhoud, wie stelt de definitie (type) en verdere afspraken vast, wie daarvoor wordt geraadpleegd, wat de wijzigingsprocedure is, wat de geldigheidsperiode is en welke beschikbare ondersteuning beschikbaar is.

Hierdoor ontstaan een catalogus van beschikbare informatieobjecten, waar deze voor wie op welke grondslag voor welk doel zijn te verkrijgen. Ook de verantwoordelijke voor de definitie ligt hier vast[40].

☞ Het werkingsgebied van E-Semantiek omvat verder:

2) Komen tot en beheren van afspraken:
- Voor bovenstaande organiseert E-Semantiek de afstemming en ondersteuning van het proces tot vaststelling. Overlegtafels worden georganiseerd langs de indeling van de informatiedomeinen. [KDA];
- Afstemming met andere ketens;
- Adviseren over in wet- en regelgeving te hanteren semantiek;

3) Beheren van referentiegegevens, codestelsels, master- of stamdata (w.o. grondslagenregister)[41] (instance niveau).

Het voorgaande impliceert dat E-Semantiek bestaat uit procedures en organisatie-elementen om de werking van E-Semantiek te realiseren.

Afspraken worden ondersteund met modellen. Voor het CDM dient methodisch aangesloten te worden op rijksstandaarden voor semantisch modelleren en op de concepten van linked-data[42]. Aanpassingen en uitbreidingen dienen tijdig plaats te vinden. In samenwerking met het programma Ketenvoorzieningen worden knelpunten en ambities verder verkend.

☞ E-Semantiek is niet de plaats voor een ketenbrede voorziening voor "melding gerede twijfel". Dit is een bedrijfsproces en overstijgt daarmee een ketencommunicatievoorziening. Hier ligt een ketensteunpuntvoorziening voor de hand in aansluiting op ondersteuning voor foutherstel.

[38] De implementatie kan gedistribueerd zijn
[39] Zie DMBOK voor de exacte definities
[40] De concrete invulling van de afspraken 3.2, 3.3. en 3.4 uit EA JenV m.b.t. betekenis en verantwoordelijke voor gegevens
[41] Het Bureau Referentiegegevens heeft een JenV-breed bereik. De strafrechtketen dient hiermee zeer nauw samen te werken.
[42] Bij de Nationale Politie is veel kennis over semantisch modelleren en linked-data.

? Punt van discussie en nader onderzoek: in welke mate draag E-Semantiek bij aan het verbeteren van de kwaliteit van gegevens? Bijvoorbeeld door het beschikbaarstellen van toetsingsinstrumenten, kwaliteitscontroles en rapportages.

7.2 Integriteit, traceerbaarheid en transparantie

Met behulp van E-Index, E-Status en E-Handtekening kunnen betrouwbare informatiesporen ("bewaar- en bewerkingsketen") worden opgebouwd. Een voorwaarde voor het vertrouwd kunnen delen en kopiëren van informatieproducten.

Deze KCV'en geven ook invulling aan de beoogde verzakelijking van Dienstoriëntatie met bijbehorende transparantie. Allereerst is dit van belang voor de correcte werking van de keten, zoals betrouwbaar inzicht kunnen geven in de voortgang aan slachtoffers, getuigen, verdachte(n), advocatuur, medewerkers, etc. Daarnaast is het van belang voor betere informatie over de keten zoals voor de strafrechtketenmonitor en onderzoek. Breuken in het proces of de tijd worden zichtbaar.

Het opbouwen van de bewaar- en bewerkingsketen is ook behulpzaam bij het herstellen van fouten. Als een fout is gemaakt kan door het volgen van de bewaar- en bewerkingsketen de verspreiding door de keten in kaart worden gebracht. Vervolgens kan in een bedrijfsproces het herstel worden aangepakt.

Het inzichtelijk maken hoe informatieobjecten door de keten stromen en het waarborgen van de integriteit en authenticiteit is een samenspel van de ketencommunicatievoorzieningen:

1) E-Index: voor unieke identificatie van informatieobjecten (personen, zaken, documenten, etc.);
2) E-Index: voor relaties tussen informatieobjecten; (persoon X is (op dit moment) verdachte bij incident 123)
3) E-Index: voor de bewerkingen op informatieobjecten tussen "origineel", "bewerkingen" en "kopieën";
4) E-Index: voor de locatie van een informatieobject (waar is het?);
5) E-Status: voor afspraken, o.a. de overdracht van zeggenschap;
6) E-Handtekening: om integriteit en authenticiteit te kunnen valideren.

E-Index, E-Status en E-Handtekening zijn de bouwstenen voor de bewaarketen, bewerkingsketen en track & trace. Het zijn ook de bouwstenen voor het informatieobject dossier[43] en het nesten van dossiers.

? Er wordt een referentiearchitectuur uitgewerkt om de opzet en werking van E-Index en E-Status te concretiseren.

☞ Een waarschuwing is op zijn plaats. De concepten achter E-Index en E-Status zijn zeer krachtig en ook verleidelijk. Het streven naar inzicht en controle kan makkelijk ontaarden in alles uniek identificeren en aan elkaar relateren en elke afspraak formaliseren. Dat leidt tot een ongewenste administratieve last, privacy-schendingen, te grote complexiteit en ruis door de hoeveelheid informatie.

7.2.1 E-Index

E-Index gaat over het vastleggen van unieke identificaties, de relaties tussen objecten, modificaties en de locaties. Welke type objecten en type relaties we onderkennen ligt vast in E-Semantiek, evenals de afspraken over nummerstelsels. Conceptueel onderkennen we vier type indexen:

Type index	Toelichting
Object-index:	Informatieobjecten en hun unieke identificatie.
Relatie-index:	Geeft de onderlinge relaties weer tussen informatieobjecten zoals personen, zaken en stukken. Hierdoor wordt het bijvoorbeeld mogelijk om in te zien welke persoon betrokken is bij welk(e) beslissing(en).
Transformatie-index:	Geeft de relaties aan van de afgeleide documenten uit het originele document. Bijvoorbeeld een fragment uit een multimediabestand of het dictum uit een vonnis. Transformatie-index is een verbijzondering van de relatie-index.
Locatie-index:	Verwijst naar de locatie van informatieobjecten met een digitaal voorkomen waaronder gestructureerde gegevens en/of stukken (pdf's, multimediabestanden).

☞ Op ketenniveau is alleen zichtbaar en bruikbaar wat op ketenniveau nodig is om over organisaties heen tot een gesloten informatieketen te komen. Zichtbaarheid en

[43] Zoals in KDA 1.0 is opgemerkt bestaat "het dossier" niet. Er zijn veel verschijningsvormen, waarbij ook de benaming niet altijd eenduidig is.

bruikbaarheid die ook tijd gebonden kunnen zijn (nog niet, niet meer, etc.). Zo zal in de opsporingsfase soms minder of andere informatie zichtbaar zijn dan wanneer de zaak onherroepelijk is geworden.

☞ In de keten wordt alleen gecommuniceerd met ketenbreed afgesproken nummers. Hiervoor is er een afgesproken en gevalideerde set aan nummerstelsels ten behoeve van de strafrechtketen welke een verbindende rol heeft binnen de strafrechtketen. Ieder nummerstelsel kent een verantwoordelijke die belast is met het beheren van unieke nummers die eenmalig worden uitgegeven. Uitgeven van unieke nummers kan centraal en/of decentraal belegd worden. Al deze afspraken liggen vast in E-Semantiek.

De strafrechtketen maakt zoveel mogelijk gebruik van bestaande en vastgestelde ketennummerstelsels (zoals SKN, SIN, en UVN[44]) en de bijbehorende voorzieningen.

☞ Voor toegestane relaties in de Relatie-Index en toegestane transformaties in de Transformatie-Index gelden dezelfde regels (verantwoordelijkheid, vastgelegd in E-Semantiek, etc.) als voor nummerstelsels.

☞ De vertaling van een organisatie-intern nummer naar een ketennummer is de verantwoordelijkheid van de betreffende ketenpartner. E-Index is hiervoor niet bedoeld. Onderliggende techniek of ontwerpen mogen uiteraard worden hergebruikt.

☞ Gebruik ketennummers, zoals bijvoorbeeld SKN, niet als primaire sleutels in interne administraties.

Oorspronkelijk was VIPS-nummer een nummer dat DJI gebruikte voor identificatie van haar bewoners (ongeacht de insluitingsgrond: straf, vreemdeling, civiel). Vervolgens is dit omgezet (rond 2000) naar VIP-nummer (en later SKN) en strafrechtketenbreed in gebruik genomen. Omdat het VIPS-nummer (tegenwoordig SKN) de sleutel was in de oude systemen van DJI kwamen ook personen zonder strafrechtelijke titel in de SKDB. [VIB]

☞ Indices hebben een onveranderlijk karakter. Wijzigen kan alleen door een nieuwe toevoeging die de vorige ongeldig maakt. Voorbeeld: als een persoon aanvankelijk als verdachte is aangemerkt en later niet meer dan verdwijnt de relatie niet maar wordt ongeldig verklaart. Alleen zo kan de strafrechtketen duurzame en betrouwbare informatiesporen opbouwen.

De indexen in een voorbeeld verkort geïllustreerd:

Er is een uniek Informatieproduct IP123. (E-Index Object-index)
Informatieproduct IP123 is van het type PV-Aangifte. (E-Semantiek)
Het type PV-aangifte kan [0 tot n] slachtoffers omvatten. (E-Semantiek)
Aan E-Index kan gevraagd worden of er slachtoffers verbonden zijn met IP123. Indien dat het geval is dan retourneert E-Index de identificerende nummers van de met IP123 verbonden slachtoffers, bv. ID A12 en B12 (Relatie-index).
IP123 meldt de unieke persoons ID's A12 en B12. (Relatie-index).
Bij ketenpartner QAZ kan vervolgens informatie over A12 en B12 verkregen worden. (Locatie-index)
Dan blijken Jansen en Pietersen de concrete personen voor respectievelijk A12 en B12 te zijn.

De weg andersom bewandelen is nu ook mogelijk. Dan kan de vraag "in welke informatieproducten van het type PV-aangifte komt A12 als slachtoffer voor" gesteld worden.

Deze manier van modelleren, gebaseerd op de concepten van het semantisch web (o.a. linked data) maken het mogelijk om van meerdere kanten (persoon, zaak, gebied, thema) vragen te stellen. Hetgeen vervolgens persoonsgericht- en zaakgericht werken mogelijk maakt.

Veel gegevens, zoals in het voorbeeld, zijn beschikbaar in de keten. Ze zijn echter niet op een gestructureerde manier te ontsluiten. De eerste stap moet zijn deze typen en relaties eenduidig te beschrijven in E-Semantiek. Daarna komt de implementatie ervan in de indexen van E-Index.

☞ Ketenpartners spreken af welke indexen nodig zijn en welke indexen voor wie met welk doel in de keten beschikbaar zijn. De ketenpartner die de index(en) beschikbaar stelt dient daarvoor zelf de technische voorzieningen te realiseren en te ontsluiten via E-Koppeling.

De verwachting is dat de implementatie van E-Index veelal decentraal zal zijn met standaard ontsluiting voor de keten.

7.2.2 E-Status

In de strafrechtketen maken de ketenpartijen veel afspraken en toezeggingen. Ondanks dat deze soms impliciet zijn gaat het in de praktijk meestal goed. Dat komt omdat er

[44] SKN =StrafrechtKetenNummer, SIN=SpoorIdentificatieNummer (forensisch onderzoek) , UVN=UniekVoorwerpNummer (beslag)

zorgvuldig wordt gewerkt en medewerkers corrigeren en trekken fouten recht. Door het impliciete karakter gaat het soms ook mis of wordt er laat op een afspraak gereageerd. Als de administratie wordt nagelopen blijkt het spoor terug slecht te volgen door incompleetheid en breukvlakken. Met het principe "Dienstoriëntatie" en het "afsprakenpatroon" worden afspraken inzichtelijk en verzakelijken deze. Op informatieniveau is E-Status de voorziening hiervoor.

E-Status maakt het mogelijk om de voortgang en status van een dienst (in termen van (b.v. laatst) gemaakte afspraak) of een proces te kennen. Eventueel kunnen derden, met behulp van het attenderingspatroon, hierover geïnformeerd worden.

E-Status geeft de toestand weer van het aangaan en nakomen van afspraken, zoals of iets beloofd, verzocht, inmiddels aanvaard, geweigerd of ingetrokken is (zie Interactiepatroon: Afsprakenpatroon). Het beschrijft de voortgang van een afspraak en niet alleen de laatste stand van zaken. De communicatie over en weer is van begin tot de huidige stand te volgen.

Wat in E-Status over afspraken wordt vastgelegd, zoals welke toestanden en statussen het betreft, de syntax waarin daarover kan worden gecommuniceerd en de wijze waarop deze informatie kan worden verkregen, ligt vast in E-Semantiek.

☞ Ketenpartners houden zelf de voortgang bij rond het nakomen van afspraken. Het vastleggen van de status van een dienst is de verantwoordelijkheid van de ketenpartner die de statusverandering in die dienst teweegbrengt.

De implementatie van de ICT voor E-Status zal decentraal ingericht zijn.

Statusveranderingen kunnen ook ontstaan door het verstrijken van de tijd. Een betekend vonnis wordt onherroepelijk als geen beroep is aangetekend in de daarvoor gestelde termijn.

☞ De verantwoordelijkheid voor het bekend maken van het verstrijken van een termijn dient belegd te zijn bij een ketenpartner.

☞ Ketenpartners spreken af welke afspraken en welke statussen voor de keten beschikbaar zijn. De ketenpartner die afspraken en statussen beschikbaar stelt dient daarvoor zelf de technische voorzieningen te realiseren en te ontsluiten via E-Koppeling.

Tot nu toe gaat de beschrijving uit van de voortgang en status van afspraken. Uiteraard kan een object een status hebben. Veelal is dat een gevolg van dienstverlening of het gevolg van gebeurtenissen die vastgelegd of verklaard zijn.

Voorbeeld
Een auto is in beslag genomen, gaat naar domeinen, is daar in beheer en vervolgens in de verkoop. Dat is te zien als statussen van het object "voertuig". Het wijst even zo goed op de diensten waaraan deze auto onderworpen is, zoals "in beslag nemen beslagobject, transporteren beslagobject, beheren beslagobject, verkopen beslagobject".

Bederfelijke waar kan in de tijd ongeschikt worden. Dat is een statusverandering van het object. In de administratieve wereld zal iemand dat moeten verklaren en vastleggen. Belangrijk voor de bewaarketen van het informatieobject.

? Het is nog te bezien of E-Status uitbreiding behoeft voor objectstatus.

7.2.3 E-Handtekening

Bij het werken met digitale stukken moeten maatregelen worden getroffen om de integriteit, bruikbaarheid, authenticiteit en betrouwbaarheid van informatie te waarborgen. Onderdelen van de in 3.2 benoemde BIVA eisen. De digitale handtekening is een middel waarmee burgers, bedrijven en andere betrokkenen de authenticiteit en integriteit van digitale stukken kunnen vaststellen. Met het vaststellen van authenticiteit van het stuk wordt bedoeld dat met een bekende mate van zekerheid kan worden vastgesteld wie de ondertekenaar van dat stuk is. De ondertekenaar kan worden geverifieerd. In de papieren werkwijze wordt dit bereikt met de "natte handtekening". Met integriteit wordt gedoeld op de zekerheid dat de inhoud van het document of de transactie volledig is en niet onbevoegd is gewijzigd of beschadigd. De handtekening richt zich op authenticiteit en integriteit. Waarmerken richt zich op de integriteit. In de papieren werkwijze wordt dit o.a. bereikt met zegels, paraferen van pagina's en watermerken. (bron Astra ABB Digitale handtekening)

☞ Van een informatieobject met rechtsgevolgen, in elke verschijningsvorm (document, film, bericht, origineel of kopie, etc.) moet de integriteit en authenticiteit vast te stellen zijn. Een digitale handtekening of waarmerk kan hiervoor nodig zijn. Dit is echter niet alleen een technische vraag. Juridische en organisatorische afspraken en waarborgen zijn nodig

! Voor het gebruik van digitale handtekening maakt de strafrechtketen onderlinge afspraken om

betrouwbaarheid van de handtekening of het waarmerk zeker te stellen Zie hoofdstuk 3.2 Digitale datasoevereiniteit over BIVA-eisen.

☞ In de ABB Digitale Handtekening [BDH] is afgesproken dat:
- Eigen implementaties voor de digitale handtekening mogelijk zijn;
- Gebruik van een gezamenlijke voorziening voor het zetten van een digitale handtekening mogelijk is;
- Er een gemeenschappelijke validatie voorziening (GAAV) is.

Voor de technische implementatie sluit de strafrechtketen aan bij Justitie- en Rijksafspraken en -standaarden.

! Te ontwikkelen: digitale handtekening/waarmerk voor andere formaten dan het huidige PDF. Denk aan multimedia bestanden, berichten. Ook dit reikt verder dan alleen een technische voorziening. Juridische en organisatorische afspraken en waarborgen zijn nodig.

? Nader te bepalen: Geldigheidsduur van een digitale handtekening/waarmerk ten opzichte van de bewaartermijnen van het getekende informatieobject. Omdat algoritmes voor hashing na verloop van tijd worden gebroken gaat GAAV uit van een geldigheid van een digitale handtekening/waarmerk van 5 jaar. Vragen zijn of een langere termijn noodzakelijk wordt[45], of vanuit digitaal archiveren aanvullende eisen ontstaan en hoe daaraan tegemoet wordt gekomen.

7.3 Technisch uitwisselen

Met KCV'en E-Koppeling, E-Distributie, E-Makelaar en E-Portalen kan informatie technisch worden uitgewisseld. Technisch uitwisselen gaat over de afspraken, standaarden en techniek, nodig om informatieobjecten tussen ketenpartners uit te wisselen: het hoe van het uitwisselen.

Om organisaties te verbinden en toch los te koppelen is er een koppelvlak per organisatie dat de interne informatievoorziening afschermt van de keten (E-Koppeling). Om koppelvlakken te verbinden zijn ondersteunende functies nodig als protocolconversie en syntaxconversie (E-Distributie). Om speciale of veel voorkomende patronen van technisch uitwisselen in de keten te vergemakkelijken zijn er ketencommunicatievoorzieningen als E-Makelaar voor opvragen en kennisgeven. Technisch uitwisselen kent alleen interactiefunctionaliteit (schermen, apps, etc.) voor beheerdoeleinden. Voor de verbinding met de veel voorkomende presentatievorm portalen zijn afspraken nodig (E-Portalen).

Het onderscheid van deze vier KCV'en is conceptueel van aard. Bij implementaties zijn combinaties mogelijk. Het conceptuele onderscheid is van belang om goed onderscheid te maken tussen verantwoordelijkheden, implicaties van digitale datasoevereiniteit, en vervolgens beheer en financiering. Wat is aan de ketenpartner? Wat is gezamenlijk? Bij implementatie dienen hier bewust keuzes gemaakt te worden.

Zo is E-Koppeling een ketenafspraak, de implementatie is de verantwoordelijkheid van de ketenpartner. Distributiefuncties, zoals schemavertaling van EBMS (strafrechtketen) naar STUF (gemeente-domein) kan iedere ketenpartner voor zich realiseren.

Gezamenlijk is efficiënter wat betreft kennis en kosten. Het kan echter strijdig zijn met de BIVA-eisen, digitale datasoevereiniteit omdat een derde partij (ICT-dienstverlener) inzicht krijgt in gegevens. Al was het maar via de logging-administratie.

Daarnaast heeft gezamenlijkheid effect op flexibiliteit. Het biedt een voorsprong door kennis en snel mee kunnen doen. Bij wijzigingen is er uitgebreidere afstemming nodig wat tot vertraging kan leiden.

☞ Voor deze KCV'en wordt zoveel mogelijk aansluiting gezocht met Rijks- en JenV-standaarden.

7.3.1 E-Koppeling

E-Koppeling is het koppelvlak tussen de ketenpartner en de keten. Op het koppelvlak wordt de taal van de keten gesproken. Zowel semantisch als technisch.

[45] De NORA gaat uit van 30 jaar.

☞ Het ontkoppelt de interne informatievoorziening van de keten. Het is de voordeur van de organisatie. Logisch gezien is er één voordeur, technisch zijn meerdere implementaties mogelijk. Wat er achter de voordeur op applicatieniveau afspeelt blijft verborgen voor de keten. Concreet: met informatiediensten wisselen we informatieobjecten uit met het OM (de organisatie van de ketenpartner), niet met GPS of NIAS (beide OM-interne IT-systemen).

Figuur 11 E-Koppeling: de I-voordeur van een organisatie

Het begrip organisatie dient nader te worden geduid en afgesproken. Een verduidelijking:

Adresseren we DJI, of maken we onderscheid per P.I., DV&O, NIFP, Zorg inkoop, etc.?
Adresseren we de Rechtspraak, of de Rechtbank Almelo of de Militaire Kamer?
Adresseren we het OM, of per afzonderlijk parket of de betreffende OvJ?

De granulariteit is afhankelijk van juridische eisen en gegevensbescherming. En dient onderscheiden te worden naar technische en logische adressering.

In het verleden is een wildgroei aan adressen ontstaan. Er zijn verschillende codestelsels binnen Justitie. Deze codestelsels en (sub)OverheidsIdentificatieNummers (OIN's) zijn uitgegeven zonder heldere afspraken wanneer een code wordt toegekend (technisch, organisatorisch, juridisch, etc.) en waarvoor deze gebruikt mag worden.

☞ Een paar vuistregels: gegevens worden logisch geadresseerd aan de verantwoordelijke juridische entiteit. (organisatorische adressering).

Een bevel behorend bij een Last Tot Ten Uitvoerlegging (LTTU) aan de Directeur van de Inrichting. (wettelijke grondslag in PBW).
Een verzoek voor een pro justitia onderzoek wordt via het NIFP toegewezen aan de gedragsdeskundige. (wettelijke grondslag voor de gedragsdeskundige in WvSv).
Technisch kunnen de verzoeken aan DJI gericht zijn. Omdat niet iedere DJI-medewerker hier kennis van de inhoud mag nemen ontstaat (een logische adressering gecombineerd met een fysieke adressering). In ouderwetse termen: envelop in een envelop.

? Nadere afspraken zijn nodig over het adresseren van organisatie en organisatieonderdelen. Bij de DI&I is een eerste aanzet beschikbaar, het Katern Justitie Actoren [KJA].

☞ Ketenpartners publiceren naar andere ketenpartijen welke organisatorische adresseringen toegestaan zijn, en welke daarvan in welke situatie te gebruiken.

☞ De ketenpartner maakt inzichtelijk welke informatieobjecten uitgewisseld kunnen worden op welke grondslag met welke doelbinding. Dit is vastgelegd in E-Semantiek. Vanaf het koppelvlak spreken we de taal van de keten, eveneens afgesproken en vastgelegd in E-Semantiek.

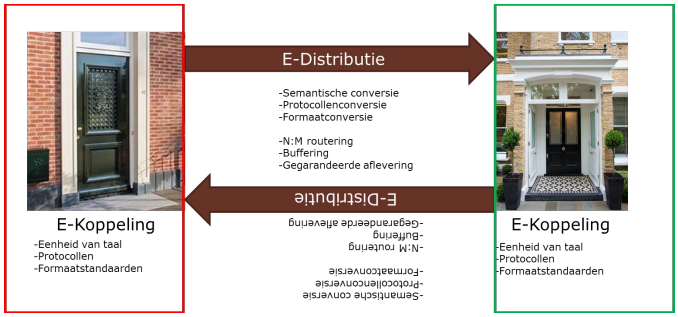
☞ Op technisch niveau maakt een ketenpartner de adressering en de wijze waarop met hem informatieobjectentypen uitgewisseld kunnen worden bekend, zowel de ondersteunde patronen (push, push/pull, etc.) als ondersteunde protocollen (berichtenverkeer, streaming, restful api, etc.). Een ketenpartner is verplicht minimaal één van alle afgesproken technische standaarden te implementeren.

7.3.2 E-Distributie

⇔ Om van voordeur naar voordeur te komen zijn soms ondersteunende functies nodig. Denk aan de in 7.3 beschreven protocolconversies.

Deze ondersteunende functies zijn onderdeel van E-Distributie. Het is de verbinding tussen de koppelvlakken van de ketenpartners. E-Distributie verzorgt de volgende functies (op basis van gemaakte afspraken in E-Semantiek en E-Koppeling):

- Conversies, vastgelegd in E-Semantiek, van syntax en coderingsstelsels;
- Conversies van technische protocollen tussen E-Koppelingen;
- Routering, inclusief "verbergen" daadwerkelijke technische locatie van een koppelvlak (ontzorgen);
- Buffering in geval van asynchrone communicatie;
- Gegarandeerde aflevering;
- Keten- of domeinbrede pseudonimisering;
- Koppeling naar standaardfunctionaliteit voor bijvoorbeeld beveiliging, loggen van verkeer (offloading).



Figuur 12 E-Distributie de verbinding tussen voordeuren

Welke distributiefuncties exact nodig zijn is afhankelijk van de afspraken over de koppelvlakken en de keten. Binnen de strafrechtketen zijn conversies van syntax en coderingsstelsels ongewenst. De strafrechtketen spreekt immers dezelfde semantische ketentaal. De conversiefuncties vormen de brug naar andere ketens als de Migratie- of Jeugdketen.

☞ De verantwoordelijkheid voor functies van E-Distributie zijn belegd. En de functies zijn getoetst aan de eisen m.b.t. BIVA, beveiliging en gegevensbescherming.

☞ De KDA bepleit gezamenlijk gebruik van E-Distributie functies. Waarbij waar mogelijk gebruik wordt gemaakt van Rijks- en JenV-standaarden en voorzieningen.

☞ Een ketenpartner kan echter beslissen een distributiefunctie onder eigen verantwoordelijkheid en beheer te houden. Voor semantische en syntactische conversie dient voldaan te worden aan de afspraken zoals vastgelegd in E-Semantiek.

☞ Bij nieuwe of vervangende informatie-uitwisseling dient minimaal aan één kant aan de nieuwe semantische en technische afspraken te worden voldaan. Daarmee wordt voorkomen dat op de oude voet verder wordt gaan.

☞ Door verschillen in standaardisatietempo tussen ketenpartners kan het nodig zijn om een tijdelijk E-Distributiefunctie te realiseren in de SRK-keten. Zoals gesteld, in 4.8.6 "Verschil in tempo en verantwoordelijkheden" is het uitgangspunt daarbij: "de vervuiler betaalt". Voor veel voorkomende tijdelijke overbruggingen kan en mag een gezamenlijke E-Distributie functie ingezet worden. Dit laatste vraagt een expliciet besluit van de alle betrokken ketenpartners met heldere afspraken over governance, financiering en uitfasering.

☞ Verantwoordelijkheid voor processen bij de ketenpartners gecombineerd met het uitgangspunt dat KCV'en, m.u.v. E-Koppeling voor interne distributie achter de voordeur, geen proceskennis mogen hebben verbieden routering van berichten op basis van de inhoud van een bericht. Ook vanuit oogpunt van gegevensbescherming is dit ongewenst. Vergelijk dit met de postbode die de inhoud van een brief moet kennen om deze af te leveren. De adressering moet voldoende zijn.

7.3.3 E-Makelaar

Conceptueel ondersteunt de E-Makelaar de interactiepatronen "vraaggestuurde informatiedeling" en "attendering". Respectievelijk met de vraagmakelaar en de notificatiemakelaar.

Conceptueel is de functionaliteit voor "attendering" strikt gescheiden en autonoom gehouden van "vraaggestuurde informatiedeling". Bij implementatie is het mogelijk deze functionaliteiten te combineren. Waarbij gebruik van de ene functionaliteit niet mag verplichten tot het gebruik van de andere functionaliteit.

De E-Makelaar, zowel vraagmakelaar als notificatiemakelaar, is een dienst geleverd door een dienstverlener. D.w.z. organisatie, mensen en software voor inrichten en configureren van de E-Makelaar.

Vraagmakelaar

De vraagmakelaar ondersteunt het vraaggestuurde interactiepatroon voor veel voorkomende, herhalende, dezelfde of gecombineerde vragen van ketenpartners, dit met de bedoeling dat "op dezelfde vraag iedereen hetzelfde antwoord krijgt"[46]. Dat wil zeggen dat het antwoord voor iedereen op dezelfde wijze tot stand komt. Bovendien dient de vraagmakelaar bij te dragen aan schaalvoordeel en efficiëntie in het applicatielandschap van de ketenpartijen: niet steeds het wiel uitvinden en realiseren. Specifieke vragen zullen niet via de vraagmakelaar verlopen, tenzij daar een goede reden voor is. De vragen die de makelaar afhandelt zijn vooraf gedefinieerd.

De vraagmakelaar staat ten dienste van de informatieafnemer. De vraagmakelaar bedient de informatieafnemer(s) door veel voorkomende samenhangende vragen in één keer te behandelen. Dit op basis van een voorafgesproken "receptuur", welke vastligt in E-Semantiek.

Een voorbeeld van zo'n vraag: Wat is het woonadres / vestigingsadres van de eigenaar, op datum dd-mm-yyyy, van de auto met kenteken x-123-

[46] Uiteraard indien geautoriseerd

abc. Dit zijn twee vragen in één. Een vraag aan het RDW voor de eigenaar van de auto, een vraag aan de BRP voor het adres van de eigenaar van de auto of het Handelregister indien sprake van een niet natuurlijk persoon. Het is mogelijk dat de vragensteller zelf de twee vragen stelt en de antwoorden combineert. De vraag kan ook gesteld worden aan de Basisregistratie Communicatie Service (BCS), die basisadministraties ontsluit. De BCS biedt dit als één standaardvraag aan met één standaardantwoord. Dit leidt niet tot een ander resultaat. De BCS heeft dus functionaliteiten als E-Makelaar in zich, naast E-Distributie (o.a. protocolconversie)

☞ De vraagmakelaar handelt onder verantwoordelijkheid van de informatieafnemer. Er zal dus, net zoals zonder de inzet van de vraagmakelaar, een gegevensverwerkingsovereenkomst moeten zijn (met grondslag en doelbinding) tussen de organisatie (dienstafnemer) van de informatieafnemer en de informatieverstrekkers. Verstrekkingen en ontvangsten worden vastgelegd bij resp. de informatieverstrekker(s) en de dienstafnemer.

☞ Daarnaast zal er een overeenkomst moeten zijn tussen dienstafnemer en de dienstverlener over kwaliteit van de dienstverlening, kosten, etc.

De vraagmakelaar kent drie varianten voor bevragen:

1. Parallelle bevraging;
2. Getrapte bevraging;
3. Afleidingsbevraging.

Ad 1) Het gelijktijdig opvragen van verschillende, van elkaar losstaande, informatieproducten op basis van eenzelfde sleutel. Vb. op het moment van aanhouden of behandelen aan de ZSM tafel het opvragen van de ID-Staat bij de Justitiële Informatiedienst en de openstaande straffen en maatregelen van diezelfde persoon. Vergelijkbaar met de huidige JIP- implementatie.
Ad 2) De output van een deelbevraging geeft input voor een nieuwe bevraging. Bijvoorbeeld de vraag: "wat is het adres van de eigenaar op datum xyz van auto met kenteken XYZ?". Een vraag eerst aan het RDW om de BSN van de eigenaar van de auto op een bepaalde datum te verkrijgen. Vervolgens met de ontvangen BSN de BRP te bevragen naar het adres.
Vergelijkbaar met BCS, die een vergelijkbare getrapte bevraging heeft voor gezinssamenstelling.
Ad 3) Op basis van de deelbevragingen wordt een 100% deterministische regel uitgevoerd. Vb. "Was persoon X op datum Y meerderjarig volgens de dan geldende jeugdwet?".

! Met deze laatste vorm van bevragen (3) zijn we zeer terughoudend omdat het risico bestaat dat impliciet verantwoordelijkheden en verwerkingsverantwoordelijkheden bij de vraagmakelaar komen te liggen die het bereik van een KCV overstijgen. Per voorgenomen implementatie van type 3 is afstemming met SRK-AR nodig.

☞ Bij bevragingen van type 2 en 3 is het zaak de gegevens nodig voor verdere bevraging of afleiding te minimaliseren.

☞ De vraagmakelaar bewaart geen gegevens, anders dan nodig voor inzicht in dienstverlening en de werking van de ICT-voorziening.

In de notitie E-Makelaar (MVP) 1.0 20210506 [EMM] is de vraagmakelaar uitgebreid beschreven.

Om voor ketenpartij(en) een relevant informatieobject samen te stellen maakt een informatieverstrekker intern vaak gebruik van vergelijkbare functionaliteit. Technisch kan de functionaliteit van de makelaar identiek zijn, het is echter geen vraagmakelaar omdat het een organisatie specifieke functionaliteit is en geen ketenfunctionaliteit. Met alle gevolgen voor verantwoordelijkheden, governance en financiering.

Notificatiemakelaar

Een organisatie kan mededelingen doen c.q. anderen attenderen of kennisgeven, zonder zich te willen, mogen of moeten bekommeren over wat de geïnteresseerde daar mee doet. Het interactiepatroon Attendering. Zie ook 4.1.3.

Het belang van de attendering ligt bij de geïnteresseerde (abonnee) en niet bij kennisgever (signaleerder) van de mededeling. De verantwoordelijkheid voor het signaleren en kennisgeven aan geïnteresseerden ligt bij de ketenpartner bij wie het signaal ontstaat. Welke eventuele opvolging de abonnee aan een ontvangen kennisgeving verbindt is geheel aan de abonnee.

De notificatiemakelaar is een afsprakenset (denk aan formaat, geldigheid, etc.) en de technische ondersteuning hiervoor. Het ontzorgt de signaleerder doordat het de notificaties verstrekt aan alle afnemers die dit mogen weten. De notificatiemakelaar werkt onder verantwoordelijkheid van de signaleerder. De geïnteresseerde dient over de technisch functionaliteit te beschikken voor het ontvangen en verwerken van een notificatie.

Notificaties zijn informatieobjecten waarvan de beschrijving is opgenomen in E-Semantiek, evenals de mogelijke grondslagen en doelbindingen voor een notificatie.

☞ Notificatieberichten zijn voldoende zinvol, duidelijk en begrijpelijk. Voorkomen moet worden dat extra verkeer ontstaat om de betekenis te achterhalen van wat een notificatiebericht inhoudt. Tegelijkertijd dient vanuit

gegevensbescherming dataminimalisatie te worden toegepast.

☞ Het nader bevragen n.a.v. een notificatie is later in de tijd dan de notificatie. Daarom dienen de aanleiding voor de notificatie (de gebeurtenis) en de actuele situatie te onderscheiden te zijn.

☞ Voor de notificatiemakelaar is een abonnementenadministratie noodzakelijk, waarin wordt bijgehouden welke organisatie op grond van welke grondslag en doelbinding geabonneerd is op welke gebeurtenissen (signalen en notificaties). Bij het aangaan van een abonnement wordt gecontroleerd op een verwerkingsovereenkomst tussen signaleerder en abonnee.

De notificatiemakelaar ontvangt signalen en zorgt er vervolgens voor dat abonnees over dat signaal actief worden geïnformeerd via een notificatie. Zij controleert daarbij de geldigheid van het abonnement.

De notificatiemakelaar verwijdert signalen na een, per signaaltype afgesproken, korte termijn. De notificatiemakelaar bewaart geen gegevens anders dan de minimaal noodzakelijke t.b.v. technische logging en verantwoording en inzicht in de dienstverlening.

☞ Verstrekkingen van notificaties en ontvangsten van notificaties worden vastgelegd conform E-Compliance bij respectievelijk de abonnee(s) en de signaleerder.

! De implementatie van dit mechanisme kan zowel per ketenpartner of met behulp van een gemeenschappelijke IT-voorziening. Beide implementatievormen dienen te voldoen aan de afspraken van notificeren. Een gemeenschappelijke IT-voorziening verandert de hiervoor genoemde verantwoordelijkheden niet. De dienstverlener van zo'n gemeenschappelijke IT-voorziening is verantwoordelijk voor correcte werking van de dienst, niet voor de inhoud.

! De notificatiemakelaar mag niet uitgroeien tot een of meerdere signaleringslijsten[47] voor de keten. Dit vraagt afweging in het bedrijfsproces. Kennis die thuishoort bij ketenpartners. Dit geldt ook voor de analyse van elkaar tegensprekende of versterkende signalen van verschillende ketenpartners. Het lijkt verstandig om voor zeer kritische signalen een ketensteunpunt, zoals beschreven in "Persoonsbeeld op maat" [POM], in te richten. Hierbij valt te denken aan lijsten met voortvluchtige of gezochte personen.

7.3.4 E-Portalen

Is voornamelijk een afsprakenset, wellicht ondersteund door technische portaal-specifieke bouwstenen en -standaarden, over hoe wij portalen realiseren. Bijvoorbeeld over gebruikerservaring en de eenvoud van aansluiting van nieuwe bronnen. Zie hiervoor de ABB Portalen [APO].

! E-Portalen is onbewust van de inhoud. Dat in tegenstelling tot bijvoorbeeld het Ketenbreed Slachtofferportaal of het Verkeersportaal, waar het wel om de inhoud gaat; dit zijn dan ook ketensteunpuntvoorzieningen en geen ketencommunicatievoorzieningen

! Er is een portalenstrategie [VIS] deze geeft aanwijzingen voor het inrichten en onderscheiden van portalen. De strategie is er op gericht om van organisatieportalen over te gaan naar doelgroepportalen waarbij de klantreis centraal staat i.p.v. de taken van de organisaties. Hierbij dient de afweging gemaakt te worden tussen indeling naar doelgroep en de noodzakelijke rechtsstatelijke verhoudingen (onafhankelijkheid).

De portalenstrategie promoot het actief brengen van informatie.

? De concretisering van de visie naar doelgroepen en kanalen is nog niet vastgesteld. Daarin moet duidelijk zijn welke doelgroepen, inclusief de eigen medewerkers van de ketenpartners, we onderkennen en via welke kanalen we deze bedienen en tot welke portalen dit leidt.

☞ Portalen beperken zich tot gebruikersinteractie. Portalen bevatten alleen presentatielogica en/of logica ten behoeve van interactie met de gebruiker. Ook houden portalen geen master- of transactiedata vast. Uiteraard moet een portaal wel logging bijhouden en mag het gebruikersvoorkeuren registreren, e.e.a. om het technisch functioneren van het portaal te monitoren.

☞ Voor het vastleggen van gebruikersvoorkeuren wordt eenzelfde, waar mogelijk gezamenlijke, systematiek gebruikt. [VIS]

7.4 Rechtmatigheid uitwisselen

Hiervoor hebben we gesproken over betekenis en bronnen, authenticiteit, integriteit en transparantie als ook over de techniek van uitwisselen. De laatste set ketencommunicatievoorzieningen gaat over het kunnen aantonen of afdwingen van de rechtmatigheid van

[47] Denk aan een lijst van voortvluchtigen of gezochte personen.

informatie-uitwisseling. Het gaat dan om vertrouwelijkheid (E-Toegang), gegevensbescherming (E-Compliance) en archivering (E-Archief).

Deze onderwerpen zijn in beperkte mate specifiek voor de strafrechtketen. We sluiten zoveel mogelijk aan bij Justitie-brede afspraken en voorzieningen en maken de strafrechtketenspecifieke eisen duidelijk. Daar waar nog geen JenV afspraken zijn, nemen we als keten het voortouw en altijd in samenspraak met de organisatie binnen het JenV-domein en maken we gebruik van het CIO-stelsel en DI&I.

7.4.1 E-Compliance

E-Compliance maakt mogelijk dat SRK-Ketenpartners kunnen verantwoorden aan autoriteiten en betrokkenen in welke mate aan wet- en regelgeving is voldaan bij het verstrekken / ontvangen van informatie vanuit de strafrechtketen[48].

Hiermee kan E-Compliance als bron optreden voor (elders) uit te voeren toetsingen, zowel op het niveau van individuele verstrekkingen, hetzij op patronen. Of daarmee het werkproces daadwerkelijk rechtmatig is verlopen valt buiten de scope van E-Compliance.

De ketenvoorziening E-Compliance zorgt voor ketenbrede afspraken over gegevensbescherming voor zover dat nodig is omdat het de afzonderlijke organisaties overstijgt. Gegevensbescherming betreft:

1) het voldoen aan wet- en regelgeving m.b.t. bescherming persoonsgegevens (AVG, WJSG, WPG[49], PBW, PW, etc.);
2) afspraken rond bescherming van gegevens van slachtoffers, getuigen, justitiabelen.

Ad 1) Organisaties zijn verantwoordelijk om aan de wet- en regelgeving te voldoen. Daartoe moet een organisatie:

- kunnen aantonen dat zij alleen informatieobjecten uitwisselt als daarvoor juridische grondslag(en) en doelbinding(en) zijn;
- vragen kunnen beantwoorden van betrokkene welke informatie over de betrokkene met wie is gedeeld op grond waarvan.

Ad 2). Het mag niet zo zijn dat als een ketenpartner afspraken maakt tot bescherming van getuigen, slachtoffers of justitiabelen een andere ketenpartner diens gegevens vrijelijk ter beschikking stelt. Zie o.a. de nota "Privacy van het slachtoffer: feit of fictie" [PVS].

? Er dienen nog ketenbreed afspraken gemaakt te worden hoe de keten gegevensbescherming (foto's, adres, etc.) van slachtoffers, getuigen, justitiabelen en professionals (o.a. advocaten) implementeert op een rechtmatige wijze.

Organisaties zijn verplicht om administraties bij te houden van verstrekte en ontvangen persoonsgegevens. In eerste instantie worden in deze administraties alleen gestandaardiseerde uitwisselingen (berichten, etc.) opgenomen. E-mail, apps, etc. vallen buiten beschouwing. Deze administraties dienen minimaal te voldoen aan de ketenafspraken.

Verstrekkingen- en ontvangstenadministraties zijn zelf ook onderworpen aan wetgeving voor gegevensbescherming. Net zoals logging voor zowel functioneel als technisch beheer.

Om deze administraties mogelijk te maken zijn referentiepunten nodig. Welke grondslagen kennen wij in de keten en welke GegevensLeveringsOvereenkomsten (GLO'en) zijn afgesproken. Die referentieverzamelingen worden respectievelijk onderhouden in het ketenbrede SRK-Juridische-Grondslagenregister (onderdeel van E-Semantiek) en in ketenbreed ontsloten SRK-GLO-Registers (onderdeel van E-Compliance).

! Voorgesteld wordt om op ketenniveau deze kritieke expertise in een netwerk te organiseren, dan wel de bestaande gremia te versterken om de specifieke kennis van gegevensbescherming in de strafrechtketen te kunnen hergebruiken zodat sneller duidelijkheid verkregen kan worden en kennis niet verloren gaat.

? Ten slotte staat de vraag open hoe om te gaan met de vraag van een betrokkene naar over hem/haar verstrekte persoonsgegevens. Beschouwt de keten dat als het probleem van de burger die de afzonderlijke organisaties af moet om het inzicht te verkrijgen of kiest zij voor het perspectief van de betrokkene, die recht heeft op hulp om de verstrekkingen en ontvangsten door de hele keten inzichtelijk te krijgen?

De implementatie van verstrekking- en ontvangstregisters is een zaak voor de ketenpartners. In de KDA is weliswaar een optie voorzien voor een gemeenschappelijk verstrekkingenregister. Gezien de consequenties voor archiveren en rechtsstatelijkheid lijkt het toepassingsgebied hier voor zeer klein.

[48] Omdat veel ketenpartners in meerdere ketens actief zijn vallen hierin ook afspraken over "schotten" tussen de verschillende ketens.

[49] WPG en WJSG worden vernieuwd en wat betreft terminologie in lijn met de AVG gebracht

Het is niet uitgesloten dat E-Compliance de landingsplaats is voor andere compliance onderwerpen waarvoor ketenafspraken nodig zijn.

7.4.2 E-Toegang

Een van de BIVA-eisen is vertrouwelijkheid. Dit is ingegeven door de eisen aan het beschermen van onderzoek en door wetgeving als de WvSv, WJSG, WPG, AVG, etc.
Om hieraan tegemoet te komen worden eisen gesteld aan het identificeren van een persoon of informatiesysteem en aan de autorisatie van personen en systemen. Samengevat eisen aan Identity en Access Management (IAM).

Hiervoor zijn Justitie-breed afspraken gemaakt over federatieve toegang en het stelsel van waarborgen daar omheen.

E-Toegang is een voorziening die identificatie en autorisatie in de keten mogelijk maakt. Het vaststellen van de identiteit van een gebruiker van de voorzieningen in de strafrechtketen kan door middel van:

- publieke inlogmiddelen (zoals DigiD, e-Herkenning);
- digitale inlogmiddelen voor beroepsgroepen (advocatenpas, UZI-pas voor zorgverleners);
- een federatiesysteem waarbij de identiteiten die een andere ketenpartner hanteert transparant zijn.

Voor autorisatie omvat E-Toegang regels en afspraken, zoals de benodigde doelbinding en grondslagen (met raadplegen van E-Compliance voor het grondslagenregister[50]) en de daaruit volgende benodigde attributen.

☞ Het uitgangspunt voor vertrouwelijkheid is "need to know". Er zijn echter situaties denkbaar, zie [IUS] dat in samenspraak bepaald moet worden wat "need to know" in een concrete situatie betekent. Vertrouwelijkheid is een balans tussen systeemmaatregelen vooraf en toezicht achteraf. In geval van nood mag een medewerker niet belemmerd worden in zijn handelen. De medewerker zal wel altijd verantwoording moeten afleggen voor het tijdelijk vergroten van zijn informatiepositie[51].

☞ Rollen en attributen nodig voor autorisatiemechanismen als RBAC en ABAC zijn beschreven in E-Semantiek. Dit betreft zowel de typebeschrijving als de toegestane waarden, zolang deze laatste niet dynamisch zijn, bijvoorbeeld zaaknummer '123'. De toepassing ligt vast in E-Toegang.

☞ Voor de diensten van E-Toegang wordt gebruik gemaakt van de JenV-brede voorzieningen. In het bouwblok Identity en Access Management is toegang uitgebreid beschreven ABB IAM. Het inrichten van federatieve toegang bij de ketenpartners reikt verder dan de strafrechtketen. Per ketenpartner buiten de keten zullen de (on)mogelijkheden voor federatieve toegang afgewogen moeten worden

7.4.3 E-Archief

Het OGB heeft de visie en scenario's voor archiveren in de strafrechtketen vastgesteld.

Zowel de visie als de scenario's benadrukken dat iedere organisatie zelf verantwoordelijk is voor de compleetheid van haar "dossiers" en archiveringsverplichtingen[52]. Er is dan ook geen sprake van ketenarchivering.

De visie maakt de kanteling van het klassieke beeld van archiveren naar Duurzame Toegankelijkheid (DUTO) [VDA].

Duurzame Toegankelijkheid begint bij het ontvangen, creëren of delen van een informatieobject. En niet pas als "de zaak gesloten is". Duurzame toegankelijkheid omvat o.a. vindbaarheid en toegankelijkheid alsook het tijdig vernietigen van informatieobjecten op basis van een vastgestelde selectielijst.

DUTO-eisen zijn de algemeen geldende eisen voor duurzame toegankelijkheid van overheidsinformatie. Zij worden toegepast volgens het 'archive-by-design-principe'. Dat wil zeggen dat het toepassen van de DUTO-eisen samenhangt met inrichtingskeuzes van een organisatie voor nieuwe informatiesystemen.

☞ Omdat de bewaartermijn mede wordt bepaald door bijvoorbeeld de wijze van afdoening of de uitspraak zijn afspraken nodig over het infomeren van andere ketenpartners over gebeurtenissen die de bewaartermijn beïnvloeden. Hiervoor kan het interactiepatroon attendering worden gebruikt.

☞ In de keten worden afspraken gemaakt over de metadata t.b.v. archiveren. De nieuwe Rijksrichtlijn Metagegevens voor Duurzaam Toegankelijke

[50] Dit hoeft geen geautomatiseerde koppeling te zijn.
[51] Denk hierbij aan voorziening als Privileged Access Management (PAM) ("Broken glass") om in geval van acute nood toch toegang tot informatie te verkrijgen.
[52] De archiefwet wijst de zorgdrager aan als verantwoordelijke. In de KDA gaan we hier gemakshalve even aan voorbij. Zie voor deze verantwoordelijke [VDA].

Overheidsinformatie (MDTO) dient geconcretiseerd te worden voor de strafrechtketen.

! Metadata t.b.v. archiveren is deels anders en overlapt deels met informatieobject-inhoudelijke (meta)data. Omdat veel organisaties in meerdere justitieketens werkzaam zijn dienen de afspraken zoveel mogelijk JenV-breed bruikbaar te zijn.

☞ T.b.v. o.a. preserveren, tekenen en waarmerken dienen JenV-brede afspraken over ondersteunde bestandsformaten te worden gemaakt. Sluit hierbij waar mogelijk aan op Rijksrichtlijnen en de standaarden van het Forum Standaardisatie.

Er zijn meerdere strategieën om invulling te geven aan archivering:

1) aan het eind van de "zaak" de "stukken" overbrengen naar een digitale archiefruimte / e-depot;
2) als een document is ontvangen of geproduceerd deze toevoegen in het e-depot (een lopend archief).

Het is aan de ketenpartner hierin te kiezen. Omdat de archieffunctie in het fundament van de brug is geplaatst, doet de KDA hierover geen uitspraken.

Op de technische laag is de archiveringsfunctionaliteit zeer beperkt strafrechtketenspecifiek.

☞ In de scenario's wordt een gezamenlijk ketenarchief, dat wil zeggen een gezamenlijke gegevensverzameling van gearchiveerde informatieobjecten, uitgesloten. [SDA]

Het is aan de ketenpartner om zijn technische archieffunctie in te richten. Een JenV-ketenpartner kan kiezen zelf een applicatie aan te schaffen en in te richten of gebruik te maken van de gemeenschappelijke voorziening van JenV, het CDD. Deze gemeenschappelijke voorziening deelt dezelfde softwarebasis. De opslag, het beheer en de toegang tot de gegevens is per organisatie(onderdeel). Er is geen gemeenschappelijke gegevensverzameling.

JenV adviseert het gebruik van CDD uit oogpunt van kosten en kwaliteit. JenV-Ketenpartners hebben zich voor CDD uitgesproken met uitzondering van de Nationale Politie. Besluit OGB maart 2021.

De dienst CDD+ stelt kennis en ervaring beschikbaar m.b.t. de complexe vraagstukken als opstellen selectielijsten, preserveren en het overbrengen naar het Nationaal Archief. [besluit CDD, CIO Raad].

☞ De archieffunctie bevindt zich, logisch gezien, achter de voordeur van een ketenpartner (in het fundament), ontsloten via E-Koppeling. Dit betekent dat een archieffunctie, zoals CDD, geen distributiefunctionaliteit mag bevatten.

De Migratieketen heeft het bewaren van documenten en de administratie hiervoor bij een derde partij belegd. Dit model, ondersteund door CDD+, gaat uit van een eenmalige opslag van het informatieobject met verwijzingen per ketenpartner, (het "vlindermodel").

☞ Gezien de discussies over rechtsstatelijkheid, volledige zeggenschap, controle over toegang tot data en dat een deel van de ketenpartners geen deel uit maakt van JenV, is dit voor de gehele strafrechtketen geen optie.

n.b. De archiefwet is van toepassing op overheidsorganisaties. Ketenpartners die geen overheidsorganisaties zijn vallen hier niet onder. Veelal is er vanuit specifieke wetgeving (vb. Wet op de geneeskundige behandelingsovereenkomst, WGBO) de noodzaak tot archiveren en verantwoorden. Wetgeving die vaak ook voor overheidsorganisaties van toepassing is.

7.5 Automatiseringsgraad

In dit hoofdstuk zijn meerdere malen relaties en controles benoemd tussen de ketencommunicatievoorzieningen. Zo is hiervoor regelmatig gesteld dat kennis bij E-Semantiek beschikbaar is of dat gecontroleerd wordt m.b.v. E-Toegang of E-Compliance. Dat wil niet zeggen dat dit altijd runtime plaats vindt of geautomatiseerd is. Vaak voldoet een controle op het moment van ontwerp en realisatie. Dat laatste geldt uiteraard niet voor E-Toegang.

Real-time controle op compliance stelt zeer hoge eisen aan de afzonderlijke en gezamenlijke informatiehuishoudingen. Een niveau waar de keten nog niet aan toe is. Voorkomen moet worden dat de keten door een niet-realistisch ambitieniveau op slot komt te staan. Tegelijkertijd vereist vertrouwen in digitalisering dat de keten stapsgewijs groeit naar een hoger niveau.

8. Transitiestrategie

In het hoofdstuk 4 Keteninformatisering en in het bijzonder in "IV organiseren in de keten" is gesteld dat voor het realiseren van de Ketendoelarchitectuur, de KDA, alleen niet volstaat. Er dient een strategie te zijn voor realisatie. In dit hoofdstuk staat die transitiestrategie centraal.

"Gericht en beheerst verbeteren en ontwikkelen in stappen."

De Ketendoelarchitectuur (KDA) beschrijft de inrichting van de keteninformatievoorziening, die de soevereiniteit van de ketenpartners niet aantast, en daarom uitgaat van minimale koppeling tussen de processen, organisaties en IV. De KDA streeft het vergroten van de interoperabiliteit en daarmee betrouwbare gegevensuitwisseling tussen de ketenpartners na en het kunnen ontsluiten van die gegevens vanuit verschillende perspectieven (o.a. persoon, 'zaak'). Verwoord in het mantra: "De strafrechtketen kan digitaal, betrouwbaar, veilig en eenvoudig gegevens over personen, 'zaken', beslissingen en bewijsmiddelen uitwisselen. Zo zijn deze gegevens vanuit ieder gewenst perspectief, binnen en buiten de keten tijdig en volledig beschikbaar, voor iedereen die ze nodig heeft en mag gebruiken, om te kunnen handelen, beslissen, leren, besturen en verantwoorden."

De transitiestrategie beschrijft een aanpak om te komen van het huidige verknoopte en inflexibele IV-landschap naar de beoogde informatievoorziening in lijn met de KDA. Dit is een proces van continue verbeteren in kleine beheerste stappen.

Dit hoofdstuk komt overeen met de notitie "Transitiestrategie" die in het OGB van mei 2021 is besproken en vastgesteld.

8.1 Transitiestrategie (KDA Perspectief)

Gericht en beheerst verbeteren en ontwikkelen in stappen.

De Ketendoelarchitectuur (KDA) beschrijft de inrichting van de keten-informatievoorziening, die de soevereiniteit van de ketenpartners niet aantast, en daarom uitgaat van minimale afhankelijkheden tussen de processen, organisaties en IV. De KDA streeft het vergroten van de interoperabiliteit en daarmee betrouwbare gegevensuitwisseling tussen de ketenpartners na en het kunnen ontsluiten van die gegevens vanuit verschillende perspectieven (o.a. persoon, 'zaak', beslissing). Verwoord in het mantra: "De strafrechtketen kan digitaal, betrouwbaar, veilig en eenvoudig gegevens over personen, 'zaken', beslissingen en bewijsmiddelen uitwisselen. Zo zijn deze gegevens vanuit ieder gewenst perspectief, binnen en buiten de keten tijdig en volledig beschikbaar, voor iedereen die ze nodig heeft en mag gebruiken, om te kunnen handelen, beslissen, leren en verantwoorden."

De transitiestrategie beschrijft een aanpak om te komen van het huidige verknoopte en inflexibele IV-landschap naar de beoogde informatievoorziening in lijn met de KDA. Dit is een proces van continue verbeteren in kleine beheerste stappen.

De transitiestrategie laat zich samenvatten in vijf uitgangspunten. Ketenpartners:

1. werken doorlopend aan het implementeren van de KDA,
2. bewaken de balans tussen tijdig doen en goed doen,
3. houden rekening met elkaars prioriteiten en beperkingen,
4. denken groot maar handelen beheerst,
5. investeren in de nutsvoorzieningen van de keten.

Interoperabiliteit

Interoperabiliteit is "de capaciteit van (soevereine) organisaties om te kunnen samenwerken gericht op het bereiken van gezamenlijke doelen".[53]

Interoperabiliteit is niet het hoogste doel, het is een voorwaarde om doelen en maatschappelijke opgaven, waar samenwerking voor nodig is, te realiseren.

Om in een keten te kunnen samenwerken is interoperabiliteit nodig van wetgeving tot informatievoorziening.

Figuur 13 Europees Interoperabiliteit Framework

De KDA en daarmee deze transitiestrategie richten zich op de semantische en technische interoperabiliteit (de onderste lagen 3 en 4) en zijn een afspiegeling van en dienen congruent te zijn met de bovenliggende lagen. De noodzakelijke inrichting en samenhang met de juridische en organisatorische lagen wordt uitgewerkt in het Duurzaam Digitaal Stelsel (DDS).

[53] Conform Europees Interoperabiliteit Framework (EIF-Raamwerk)

8.2 1 - Ketenpartners werken doorlopend aan het implementeren van de KDA

Waarom:
De huidige informatievoorziening is een belemmering voor het implementeren van wetgeving, verbeteringen in de keten (zoals dienstverlening, papier uit de keten) en voor het verstrekken van samenhangende informatie bijvoorbeeld aan slachtoffers.
De huidige verknoopte, inflexibele informatievoorziening zorgt voor breukvlakken en uitval in de keten, is foutgevoelig en arbeidsintensief. Onjuiste bronnen worden geraadpleegd. Betrouwbaarheid van gegevens behoeft verbetering. Daarnaast zijn aanpassingen kostbaar en tijdrovend. Bestaande afspraken worden slecht nageleefd.

Wat:
Vergroten interoperabiliteit door losser koppelen van de informatievoorziening conform ketenafspraken, en -standaarden en ict-voorzieningen.
Conform de KDA vereist dit ook duidelijke belegging van verantwoordelijkheden en procesuitvoering.

Hoe:
De KDA is een bestemmingsplan dat richting geeft en kaders stelt aan elke verbouwing van de informatievoorziening die de keten beïnvloedt.
Projecten en programma's worden getoetst op hun bijdrage aan het bestemmingsplan en het voldoen aan de kaders.
Er wordt toegezien op het nakomen van afspraken.

8.3 2 - Ketenpartners bewaken de balans tussen tijdig doen en goed doen

Waarom:
Bij spanning tussen enerzijds tijdig resultaat halen (vb. tijdig de wet implementeren) en anderzijds kwalitatief de goede oplossing neerzetten (interoperabel, voldoen aan compliance) wordt in de praktijk veelal gekozen voor tijdigheid[54]. Lastiger werk dat de kwaliteit verbetert wordt uitgesteld, waarbij uitstel veelal afstel wordt. Dit leidt tot minder goed passende oplossingen, die weer aanleiding kunnen geven tot aanpassingen in beleid of wetgeving. Hier ontstaat opnieuw dezelfde spanning, waarbij tijdigheid weer leidend is ten koste van kwaliteit. Dit is de negatieve spiraal van afnemend aanpassings- en ontwikkelvermogen.

Figuur 14: Negatieve spiraal van afnemend vermogen

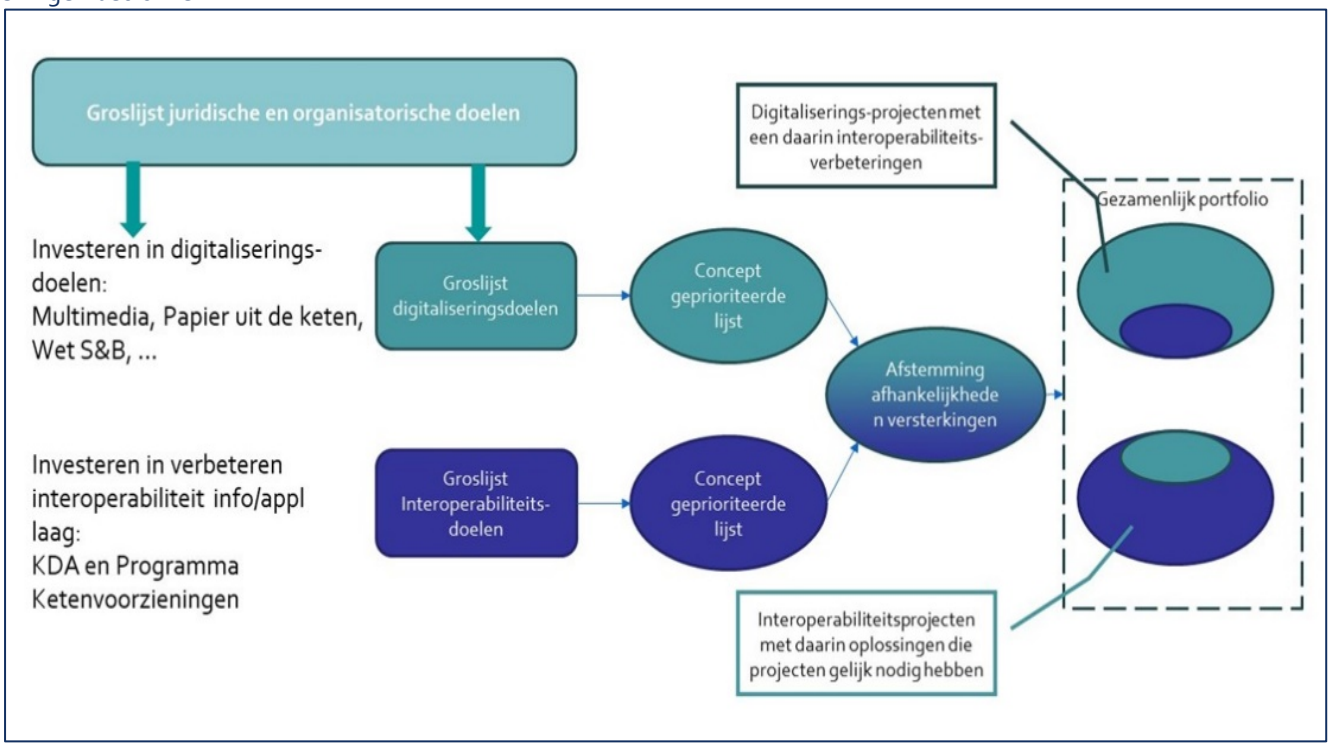
Wat:
Beter balanceren tussen tijdig en goed. Verbeteren interoperabiliteit gaat gelijk op met het realiseren van digitaliseringsdoelstellingen. Projecten dragen bij aan verbeteren van de interoperabiliteit. Prioriteit van investeringen in interoperabiliteit wordt medebepaald door behoefte en urgentie. (*Figuur 15*)

Hoe:
Het vergroten van de interoperabiliteit van informatievoorzieningen wordt één van de ketendoelstellingen.
Ketenpartners monitoren en evalueren de afgesproken interoperabiliteitsdoelstellingen. Regie op de doelstellingen is ketenpartner overstijgend ingericht.
Bij het samenstellen van het portfolio wordt de inspanning gericht op het vergroten van de interoperabiliteit met bijbehorende financiering geoormerkt.
Dit kan door projecten opdracht te geven interoperabiliteits-doelstellingen te realiseren of de weg te banen voor toekomstige businessdoelstellingen.
Hiertoe wordt een portfolioproces ingericht dat een voortschrijdend ketenjaarplan opstelt (uitgangspunt 3), vaststelling door het OGB.

[54] Notitie positionering SRK-AR (OGB feb. 2021) [PAR]

In dit proces zijn minimaal business (juridisch en organisatie), CIO-offices, portfolioraad en SRK-AR i.s.m. programma ketenvoorzieningen betrokken.

Exacte vorm wordt in samenspraak met DDS opgesteld.



Figuur 15: Balanceren van interoperabiliteitsdoelen en digitaliseringsdoelen

8.4 3 - Ketenpartners houden rekening met elkaars prioriteiten en beperkingen

Waarom:
In de keten strijden de organisatiedoelstellingen en -opdrachten (verticale krachten) en de ketensamenwerking en –doelen (horizontale krachten) om aandacht. Ketenpartners zijn actief in meerdere ketens. Dat leidt tot verschil in prioriteiten tussen ketenpartners.

Diezelfde organisaties verschillen in omvang, capaciteit en mogelijkheden van de eigen informatievoorziening. Dat leidt tot verschillen in realisatietempo en absorptievermogen.

Omdat besluitvorming over projecten op meerdere plaatsen plaatsvindt is de som van alle projecten samen vaak groter dan de individuele organisaties aankunnen. Projecten komen tot stilstand of vertragen door gebrek aan afgestemde planning waardoor de spiraal van afnemend aanpassings- en ontwikkelvermogen wordt versterkt.

Wat:
Creatief omgaan met schaarste door realistische (haalbaar en maakbaar) planning en monitoring van digitaliserings- en interoperabiliteitsdoelen.

Hoe:
In te richten: rollende meerjarenplanning en coördinatie (portfolio) over de gehele keten ("van incident tot en met interventie"). Waarbij met potlood voor de komende 3 jaren wordt gepland en met concrete afspraken voor het eerste jaar. Deze planning en coördinatie is aangesloten op de interne planning en coördinatie van de ketenpartners.

Ketenpartners helpen elkaar onder het motto "alleen ga je sneller, samen kom je verder".
Ketenpartners zijn tijdig transparant over (on)mogelijkheden, versnellingen en vertragingen.

8.5 4 - Ketenpartners denken groot maar handelen klein

Waarom:
Grote plannen, programma's en ontwerpen zijn olietankers die zich moeizaam laten bijsturen. Bijsturen kost veel tijd en geld. Vaak drijft een project af van de bestemming omdat niet tijdig gereageerd kan worden op nieuwe inzichten of veranderde prioriteiten, waardoor het middel doel wordt. Kleine projecten leveren sneller resultaat en bieden daardoor ruimte voor leren en verbeteren. Ook geven kleine projecten minder risico's en zijn beter bij te sturen.

Wat:
Groot denken en in kleine stappen gericht en beheerst verbeteren.

Hoe:
Deel verbeteringen op in kleine projecten.
Accepteer dat het niet in één keer voor elkaar is. Volgende verbeteringen worden in het portfolioproces ingebracht.
De SRK-AR ontwikkelt niet meer architectuur dan nodig is voor de komende projecten en programma's. Geen grand design.
Deze aanpak vraagt een bestemming (uitgangspunt 1) en coördinatie (uitgangspunt 2).

8.6 5 - Ketenpartners investeren in de nutsvoorzieningen van de keten

Waarom:
Kennis en besluitvorming rond ketenvraagstukken wordt veelal ad-hoc en per project georganiseerd, vaak zelfs per koppelvlak.
Besluitvorming is traag door onduidelijke adviserings- en beslissingslijnen.
Ondersteuning, leren van en kennisbehoud zijn zeer matig ontwikkeld. Het zijn dure wielen die opnieuw worden uitgevonden en daardoor hebben die wielen steeds een andere bandmaat en zijn daarmee beperkend voor de interoperabiliteit. Dit draagt weer bij aan de spiraal van afnemend vermogen.

Wat:
Kennisdeling, besluitvorming en ondersteuning zijn structureel georganiseerd ten behoeve van projecten en verbeterinitiatieven.

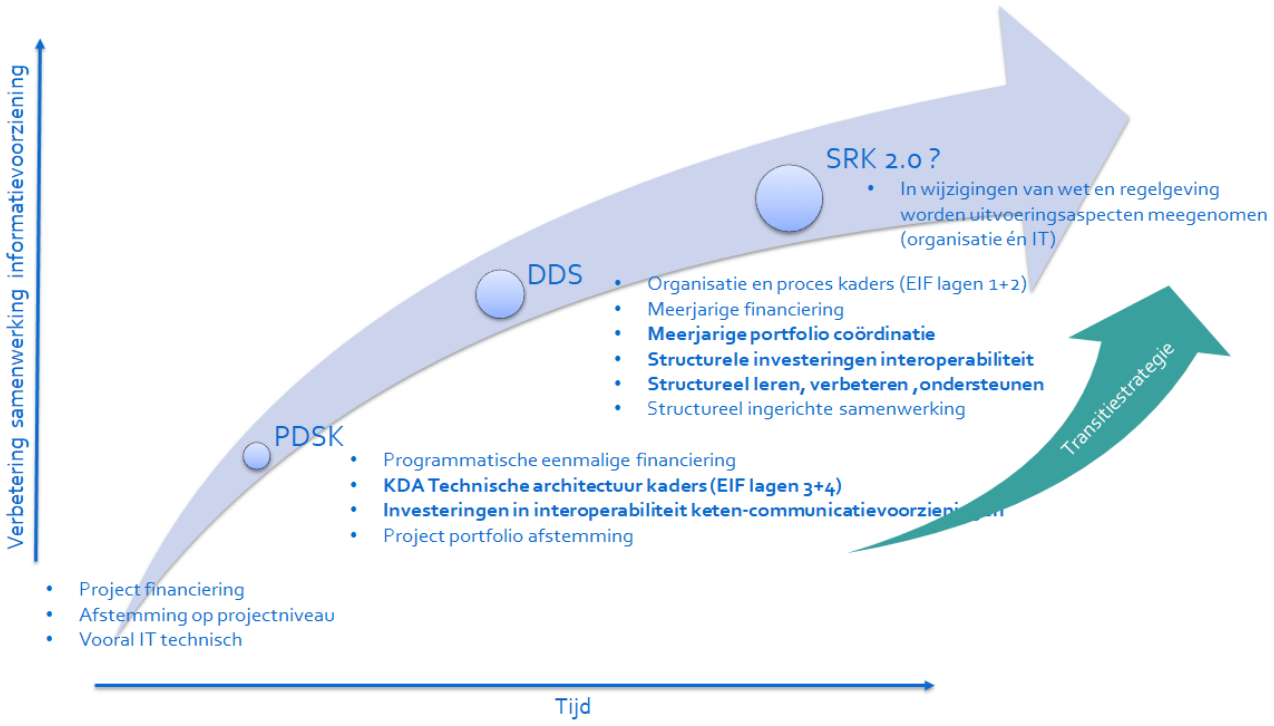
Hoe:
De KDA benoemt elf ketencommunicatievoorzieningen (KCV'en). Deze voorzieningen zijn een mix van afspraken, standaarden en ICT. Deze zullen op een soepel georganiseerde werkwijze beschikbaar moeten zijn voor projecten. Deze ondersteuning (inhoud, proces en mensen) noemen we een 'nutsvoorziening'.
Deze nutsvoorzieningen zijn daarmee de ondersteuning, het geheugen en de bron voor kennisdeling in de keten.

Nutsvoorzieningen werken samen met vergelijkbare initiatieven in andere ketens.

Ketenpartners stellen afgesproken capaciteit (kennis, tijd geld) beschikbaar voor het realiseren van de interoperabiliteitsdoelstellingen.

8.7 Transitiestrategie in perspectief

De SRK-AR ziet de transitiestrategie als onderdeel van een ketenbrede verbetering van de samenwerking. De transitiestrategie dient ingebed te worden in DDS.



Figuur 16: Transitiestrategie KDA als onderdeel verbetering informatievoorziening

Bijlage 1: Aandachtspuntenlijst

Dossiers, opbouw, overdracht, zeggenschap, nader uit te werken.

Mogelijke transformaties van informatieobjecten: tekst naar gestructureerd bericht, kopie, gewaarmerkt afschrift. Inclusief juridische/wettelijke borging.

Afschermen persoonsinformatie slachtoffer, getuigen, justitiabelen en anderen.

Relatie andere architecturen: de relatie met Europese initiatieven, kaders en voorzieningen.

Ketensteunpuntvoorzieningen:
Nader onderscheid en definities geven.

Ontsluiting van formele registers mogelijk om de actualiteit van professionals te valideren. Voorbeeld hiervan zijn: tolkenregister, deskundigenregister, BOA-register, advocatenregister.

Geldigheidsduur van een digitale handtekening / waarmerk ten opzichte van de bewaartermijnen van het getekende informatieobject.

Referentiearchitectuur voor de opzet en werking van E-Index en E-Status.

Concretisering doelgroepen en kanalenstrategie.

Informatiebeveiliging: Extra veiligheidseisen / security / classificatie
- Hoe ketenbreed om te gaan met geclassificeerde informatie.
- Vernieuwing en eisen vanuit de WJSG en WPG.

Uitkomsten van het onderzoek naar staatsrechtelijke soevereiniteit.

Statistische bewerkingen en analyses. Mede i.c.m. pseudonimisering.

Uitspraak doen over maximaal aantal toegestane versies van standaarden / afspraken (N, N-1, N-2)?

'Non functionals'
- Wat te doen als uitwijk? (uitval netwerk, stroom, servicevensters)
- Noodzaak tot 24 uurs dienstverlening
- Backup en recovery in de keten

Bijlage 2: Referenties, afkortingen en lijst met figuren

Afkorting	Bron	Auteur	Versie / datum
AMD	Attributie, mandaat en delegatie	VNG	2016
BDS	Advies borgen digitale soevereiniteit SRK	L. Moerel/ P. Timmers	4 augustus 2020
BDH	ABB Digitale Handtekening	SRK-AR	Februari 2020
BIO	Baseline informatiebeveiliging overheid	VNG	Versie 1.04_6 januari 2020
CAJ	Cloudafwegingskader JenV	Ministerie JenV	December 2019
CBB	Catalogus BAG	Ministerie BZK	2018
DDK	De digitale kooi	Kafka Brigade (A. Witlak)	2018
DDS	Duurzame samenwerking in de strafrechtketen	Ketenpartners, Ministerie JenV	Oktober 2015
EMM	E-Makelaar (MVP) 1.0 20210506.docx	SRK-AR	Mei 2021
EIF	The new European Interoperability Framework | ISA²	Europese Commissie	2017
ISV	Informatie-uitwisseling in domein overstijgende samenwerkingsverbanden	Ministerie JenV/ DGSenB	Februari 2019
HGT	Historische gegevens en Tijdreizen	Programma USB	September 2018, versie 1.0
JEW	Jegens en wegens	W. Borst	
KDA	KetenDoelArchitectuur	SRK-AR	Versie 1.0 Oktober 2020
KDB	Ketens de Baas	NORA	
KEB	Rapport Knelpunten en breukvlakken in de strafrechtketen	Ministerie JenV/DGRR/DVB/KIV	Januari 2018
KIBV	Kaderdocument informatiebeveiliging ministerie Justitie en Veiligheid	Ministerie JenV	Versie 0.41_7 juni 2019
KJA	Katern Justitie Actoren	Ministerie JenV/DI&I	Oktober 2019
KKB	Keteninformatisering in kort bestek	J.H.A.M. Grijpink	2016, 3e druk
LPD	Leidende principes Digitalisering Strafrechtketen	OBG & BKB	Versie 1.1_januari 2020
MDP	Memorie van toelichting Digitale Processtukken	Ministerie JenV	November 2014
PAR	SRK-AR: Notitie positionering	SRK-AR	16 februari 2021
PKCV	Positionpaper Ketencommunicatievoorzieningen	SRK-AR	Maart 2021
PVS	Privacy van het slachtoffer – feit of fictie?	Slachtofferhulp Nederland	2020
RGK	Raamwerk Gegevenskwaliteit	Ministerie JenV	2015
RIO	Rapport iOverheid	WRR	15 maart 2011
SDA	Scenario's digitale archivering	Project Digitaal Archiveren	28 januari 2021
TSRP	Toekomst van de strafrechtspleging	Commissie van den Emster	TSRP
VDA	Visie Digitaal Archiveren	Project Digitaal Archiveren	2020
VIB	Verdachte in de digitale bak	W. Borst	2021
VIK	Verdachte in de Ketens	W. Borst	2019
VIS	Visie IV Strafrechtketen	Ministerie JenV	2016
W@W	Werk@Wijzer	Programma USB	

Afkortingen

Afkorting	Uitgeschreven
ABAC	Attribute Based Access Control
AVG	Algemene verordening gegevensbescherming
BAG	BasisAdministratieGebouwen
BIO	Baseline Informatiebeveiliging Overheid
BIVA	Beschikbaarheid, Integriteit, Vertrouwelijkheid, Authenticiteit
BKB	BestuurlijkKetenBeraad Strafrechtketen
BRP	BasisRegistratiePersonen
CBE	Coördinerend Beraad Executie
CDM	Canoniek DataModel
DDS	Duurzaam Digitaal Stelsel
DNO	DienstenNiveau-Overeenkomst
DSK	Directie Strafrechtketen
DUTO	Duurzaam Toegankelijk
DVO	DientVerleningsOvereenkomst
GEB	Gegevensbeschermings¬EffectBeoordeling
GLO	GegevensLeveringsOvereenkomst
IAM	Identity and Access Management
JANC	Juist / Actueel / Nauwkeurig / Compleet
KCV	KetenCommunicatieVoorziening
KDA	KetenDoelArchitectuur
KSP	KetenSteunPunt
LTTU	Last Tot Ten Uitvoerlegging
MDTO	Metagegevens voor Duurzaam Toegankelijke Overheidsinformatie
MECE	Mutually Exclusive and Collectively Exhaustive
NFI	Nederlands Forensisch Instituut
NIFP	Nederlands Instituut voor Forensische Psychiatrie en Psychologie
OGB	OpdrachtGevers Beraad
PBW	Penitentiaire Beginselen Wet
PI	Penitentiaire Inrichting
PR	PortfolioRaad
RBAC	Roll Based Access Control
SIN	SpoorIdentificatieNummer
SKDB	StrafrechtKetenDataBase
SKN	StrafrechtKetenNummer
SRK	StrafRechtKeten
SRK-AR	Strafrechtketen ArchitectuurRaad
UVN	Uniek Voorwerp Nummer
WGBO	Wet op de geneeskundige behandelingsovereenkomst
WJSG	Wet Justitiële en Strafvorderlijke Gegevens
WPG	Wet PolitieGegevens
WvSv	Wetboek van Strafvordering

Overzicht figuren

Bijlage 3: Attributie, mandateren en delegeren [KJA]

Creatie en toewijzing van Publieke Taken

Voor publiekrechtelijke organen geldt het legaliteitsbeginsel[55]; Dit beginsel betekent onder meer dat alle overheidsacties moeten berusten op wettelijke gecreëerde en toegekende bevoegdheden[56]. Dit betreft zowel om privaatrechtelijke als publiekrechtelijke bevoegdheden. Hierbij geldt dat de verantwoordelijkheid voor de uitvoering van publieke taken in beginsel bij de Ministers ligt[57].

Een publieke taak[58] ontstaat en wordt toegekend door Attributie;

Attributie: (/Deconcentratie[59])	Een nieuwe bevoegdheid wordt gecreëerd, en direct toegekend aan een bestuursorgaan. Dit wordt de originaire bevoegheidsverklaring genoemd en is de enige manier waarop een nieuwe bevoegdheid kan ontstaan.

Vaak wordt de publieke taak echter door een ander orgaan uitgeoefend. Hiervoor moet de taak (gedelegeerd of) gemandateerd worden:

Delegatie:	Een geattribueerde bevoegdheid kan worden gedelegeerd naar een ander bestuursorgaan. Delegatie is een bijzonder vorm van overdracht en vereist een wettelijke grondslag; Bij delegatie verliest het oorspronkelijk orgaan de bevoegdheid tot uitoefening van de taak. De bevoegdheid wordt beperkt tot het stellen van beleidsregels, waarvan de gedelegeerde mag afwijken. De gedelegeerde mag ook eigen beleidsregels stellen. Delegatie wijzigt dus de ministeriële verantwoordelijkheid. Een voorbeeld van delegatie is bijv. het toewijzen van de publieke taak '*dragen voor de organisatie van alsmede de verlening van rechtsbijstand'* aan het Zelfstandig Bestuursorgaan (ZBO) de Raad voor de Rechtsbijstand.
Mandatering:	Een geattribueerde bevoegdheid wordt ***namens*** het bestuursorgaan *uitgevoerd* door een andere organisatie. Mandatering is een veel zwakkere vorm van verkrijgen van bevoegdheden en kan in theorie mondeling plaatsvinden. Het oorspronkelijke orgaan behoudt immers zelf de bevoegdheid, kan aanwijzingen geven en de taak wordt nog steeds in diens naam uitgevoerd. Mandatering wijzigt niet de ministeriële verantwoordelijkheid. Een voorbeeld van mandatering is bijvoorbeeld het laten uitgeven en beheren van het strafrechtketennummer door het dienstonderdeel Justitiële Informatie Dienst (Justid) namens DG-RR.

1.2 Bestuursorganen versus Taakorganisaties.

Publieke taken worden dus toegekend aan Bestuursorganen, welke hiermee het 'bevoegd gezag' vormen voor de betreffende publieke taak, en hiervoor de volledige verantwoordelijkheid dragen.

In beginsel zijn dit voor het Ministerie van JenV onze bewindspersonen. Bevoegdheden kunnen echter ook direct toegeschreven aan de hoofden van de beleidsdirecties, aan zelfstandige bestuursorganen (ZBO's) of onze Sui Generis organisaties.

Deze bestuursorganen zijn hiermee het bevoegde gezag. In de praktijk wordt vervolgens zo'n taak gemandateerd aan het Hoofd van een taakorganisaties. Deze is dan vervolgens belast met de executie van deze taak, *namens* het bevoegde gezag.

Bron: Katern - Justitie Actoren, Min JenV / DI&I, okt 2019 [KJA]

Zie ook het VNG rapport Attributie, mandaat en delegatie.

[55] Het 2de element van het legaliteitsbeginsel is dat wetten niet met terugwerkende kracht mogen werken; dit is echter hier niet relevant.
[56] NB dit kan eventueel ook op basis van een algemene wettelijk taak zijn.
[57] Zie https://www.denederlandsegrondwet.nl/id/vkugbqve7sy6/artikel_42_ministeriele
[58] Een publieke taak is een 'een *taak die in het algemeen belang wordt uitgevoerd'*.
[59] Indien de gecreëerde bevoegdheid door de Minister direct wordt toegekend aan een ondergeschikte, zoals bv een Inspecteur-Generaal, spreekt men van deconcentratie.