iKaders

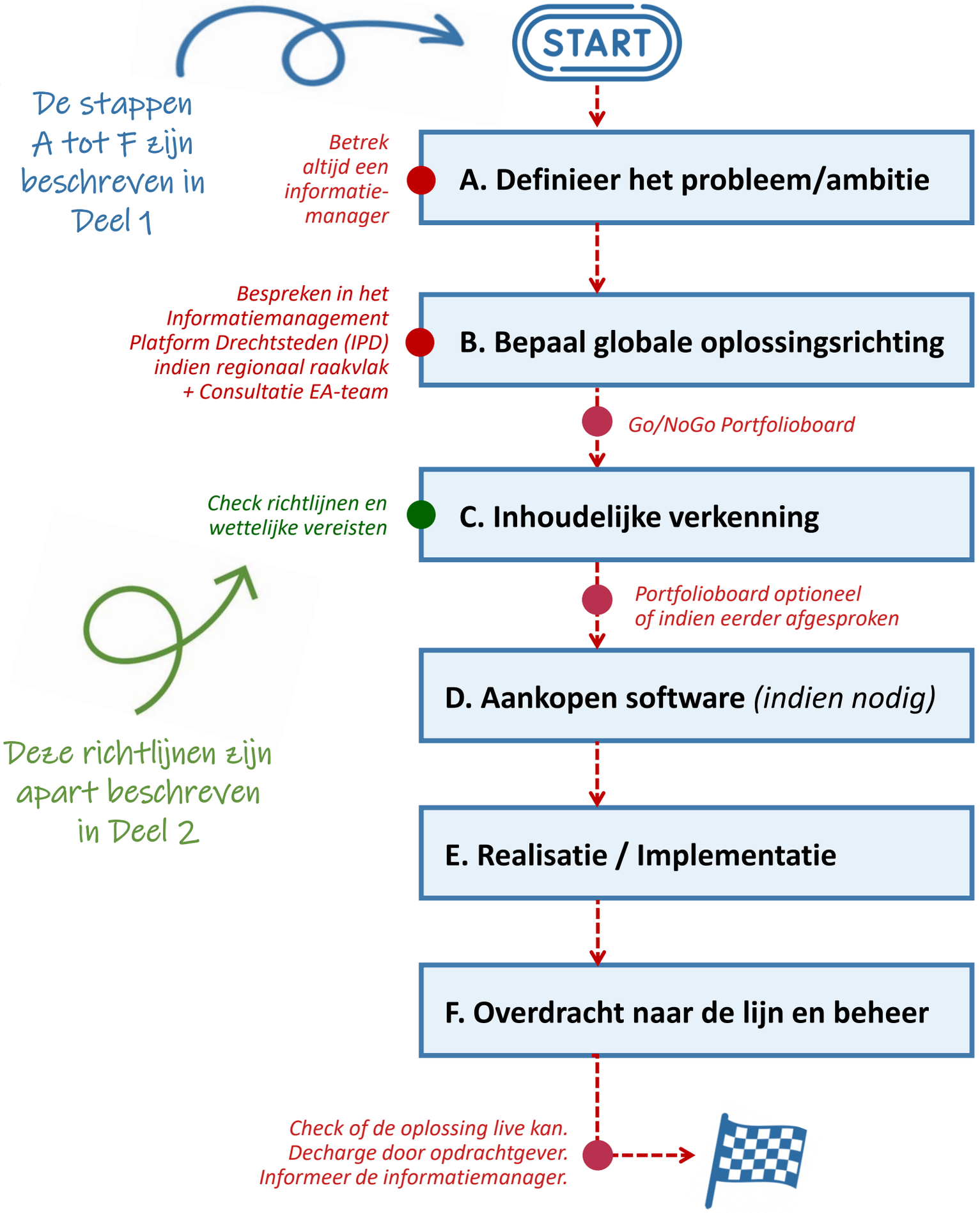
Samengesteld door M. Koopman | versie 12 | 27-5-2025
Bron: https://sid.drechtsteden.nl/Project/iKaders/Pages/wvDWNOf2tE2H_FaLchj1ew
(of ga naar SID en zoek in Groepen op "iKaders")

Introductie:
De iKaders zijn uitgangspunten en richtlijnen voor alle initiatieven met een digitaal component. Het beoogt een samenhangend overzicht te bieden dat:

- praktisch toepasbaar is voor projecten en veranderopgaven;
- zich richt op de essentie van wat goed geregeld moet worden;
- voorspelbaar maakt wanneer je met welke richtlijnen en (wettelijke) vereisten je te maken krijgt.

Hiermee regelen we:

- het veilig en verantwoord werken met gegevens, inclusief het uitwisselen, hergebruik, bewaren en archiveren;
- bescherming van persoonsgegevens en de privacy van personen;
- dat applicatie-functionaliteit niet onnodig dubbel wordt gerealiseerd;
- dat nieuwe applicaties logisch kunnen worden ingepast in het geheel van de informatievoorziening;
- dat applicaties voldoen aan het sourcing- en inkoopbeleid, en aan de vereiste technische criteria.



iKaders Deel 1

Wat in elke stap goed geregeld moet worden.

Inhoudelijke aandachtspunten bij elke (project)stap:

A. Definieer het probleem of de ambitie

START

Formuleer de ambitie of het probleem, een definitie van succes, raakvlak met strategisch/tactische doelen, afhankelijkheden met andere ontwikkelingen, en of er in het land of in de regio vergelijkbare initiatieven zijn.

B. Bepaal de globale oplossingsrichting (grofmazig)

Bepaal de **globale oplossingsrichting**. Stel zo nodig een businesscase op, en check op bestuurlijke belemmeringen. Laat je door een informatiearchitect of technisch architect helpen bij het schetsen en vormgeven van de oplossing d.m.v. een **globale architectuurschets**. Architecten gaan o.a. na of er in de Drechtsteden-regio al beproefde oplossingen zijn, en waar gebruik kan worden gemaakt van generieke c.q. standaard oplossingen.

Check de richtlijnen en wettelijke vereisten uit Deel 2.

C. Inhoudelijke verkenning van de oplossing

Bepaal de precieze **eisen en wensen voor de oplossing**, zowel technisch als functioneel, en ga na welke (**wettelijke**) **kaders** van toepassing zijn. Zet acties uit tot het vervaardigen van de benodigde stukken.

D. Aankopen software *(indien nodig)*

Leveranciers worden gekozen op objectieve gronden, en elk inkooptraject heeft een welgekozen **inkoopstrategie**. Bepalingen zijn vastgelegd in de algemene Inkoopvoorwaarden Drechtsteden. Aandachtspunten:

- Vul het **inkoop-startformulier** op intranet in (indien niet eerder gedaan).
- Stel een **verwerkersovereenkomst** op, zo nodig een **Service Level Agreement** (SLA), een **Programma van Eisen** (bij aanbestedingen), en een **afwijkadvies** (indien nodig).

Controleer of je aan de richtlijnen en wettelijke vereisten uit Deel 2 voldoet.

E. Realisatie / Implementatie

Richt de oplossing in, en implementeer deze (voor projecten) conform een eerder door de projectleider of projectverantwoordelijke opgesteld projectplan. Houdt hierbij rekening met de architectuur en alle geldende kaders en wet- en regelgeving (zie Deel 2). Betrek vroegtijdig de lijn en de toekomstige beheerders van de oplossing. Tref voorbereidingen voor de volgende stap en houdt ook rekening met de financiële consequenties na oplevering.

F. Overdracht naar de lijn en naar beheer

Maak zo nodig een **plan of draaiboek** voor de livegang, en zorg dat er **aantoonbaar** voldaan is aan alle eerder onderkende en gestelde bepalingen/eisen/richtlijnen. Betrek tijdens de realisatiefase tijdig de technisch- en functioneel beheerders om de oplossing in productie en in beheer te krijgen; dit is rand voorwaardelijk om in productie te kunnen.

Aandachtspunten in het voortbrengingsproces:

- Betrek altijd een **informatiemanager** van je organisatie.
- Leg het vraagstuk, geschatte grootte, maatschappelijke waarde en inschatting van de haalbaarheid vast in een intakedocument.
- De **informatiemanager** meldt nieuwe ambities en projecten in de dop (periodiek) aan bij de **portfoliomanager** van IDR Email: *portfolio@drechtsteden.nl*.
- Betrek zo nodig een **business consultant** van IDR.

- Ga verder met de intake en laat je voor de oplossingsrichting adviseren door de architecten en door het z.g. Enablement Team (a.k.a. **EA-team**). Zij denken mee en geven advies. Email: *eateam@drechtsteden.nl*
- Laat initiatieven naar inzicht van de informatiemanager bespreken in het **Informatiemanagement Platform Drechtsteden** (IPD) teneinde e.e.a. regionaal op te pakken.
- Stel bij grote projecten op dit moment een **projectleider** aan, en het is soms ook aan te raden alvast een inkoopstartmelding te doen. Betrek Inkoop ook bij eventuele marktverkenningen.

Bespreek het voorstel in de **Portfolioboard** voor een Go/NoGo indien een van deze situaties van toepassing is:

- het voorziene project heeft inzet of resources van IDR nodig;
- er is financiering voorzien vanuit het regionale (RPP-)budget;
- getoetst moet worden hoe e.e.a. zich verhoudt tot de lange termijn visie/beleid.

De **portfoliomanager** zal vragen vooraf een checklist in te vullen.

Stel een (consequentie-)document op waarin alles uit de inhoudelijke verkenning samenkomt. Als het een project wordt, stel dan niet later dan dit moment een **projectleider** aan. Betrek ook de mensen die de oplossing naderhand moeten gaan beheren.
Win zo nodig **juridisch advies** in bij JKC (via Weten en Regel op SID).

Optionele bespreking in de **Portfolioboard** als de inhoudelijke verkenning daar aanleiding toe geeft, of als dit eerder in de Portfolioboard is afgesproken.

Betrek vooraf **afdeling Inkoop** bij de aankoop van software of wanneer je voor de eerste keer met potentiële leveranciers in gesprek gaat.

Check of de oplossing live kan, gevalideerd en geaccepteerd is, en dus in productie kan worden gezet. Informeer de **informatiemanager**.
Hij of zij kan de **portfoliomanager** op de hoogte stellen. Nu kan ook de opdrachtgever de projectleider decharge verlenen.

iKaders Deel 1 - De afzonderlijke (project)stappen inhoudelijk nader toegelicht

A. Definieer het probleem of de ambitie

START

Zet het volgende op een rijtje:

- wie de **initiatiefnemer** en/of **opdrachtgever** is;
- wat de **ambitie of het probleem** is, zo concreet mogelijk onder woorden gebracht, met een definitie van hoe succes eruit ziet;
- raakvlakken met strategisch/tactische organisatiedoelen;
- de **afhankelijkheden** met andere ontwikkelingen en welke wetgeving
- of er in het land of in de regio **vergelijkbare initiatieven** zijn: is er een mogelijkheid om samen op te trekken of van elkaar te leren?

B. Bepaal de globale oplossingsrichting (grofmazig)

1. Bepaal de **globale oplossingsrichting**, in deze volgorde:
   - wat kan of moet er in het proces worden opgelost?
   - wat kan er worden opgelost door handiger om te gaan met gegevens?
   - wat moet er met applicaties worden opgelost?
2. Ga na of er elders (ook in de regio) al **beproefde oplossingen** zijn. Is het mogelijk samen op te trekken?
3. Ga na of er **budget** is, maak zo nodig een **businesscase** t.b.v. de besluitvorming, en check op bestuurlijke belemmeringen.
4. Laat je door een informatiearchitect of technisch architect helpen bij het schetsen en vormgeven van de oplossing d.m.v. een **globale architectuurschets**. Een architectuurschets helpt bij het inzichtelijk maken van alle benodigde IT-componenten in samenhang. Architecten gaan o.a. na of er in de Drechtsteden-regio al beproefde oplossingen zijn, en waar gebruik kan worden gemaakt van generieke c.q. standaard oplossingen.

C. Inhoudelijke verkenning van de oplossing

1. Bepaal de **eisen en wensen voor de oplossing**, zowel technisch als functioneel, en ga na welke **(wettelijke) kaders** van toepassing zijn (zie Deel 2). Zet acties uit tot het vervaardigen van de benodigde stukken door de juiste adviseurs.
2. Het is verplicht in beeld te brengen welke gegevens binnen het proces worden verwerkt:
   - Laat door een informatiebeveiligingsspecialist een **dataclassificatie** en **risicoanalyse** opstellen. *(Wettelijk kader: BIO, NIS2)*
   - Laat door de privacy coördinator een **advies m.b.t. tot de privacy aspecten** opstellen en volg de aanbevelingen uit het advies op. *(Wettelijk kader: AVG)*
   - Team DIV (Documentaire Informatie Voorziening) helpt met het uitvoeren van een **informatieanalyse**. *(Wettelijk kader: Archiefwet)*

D. Aankopen software *(indien van toepassing)*

1. Verzamel alle stukken en maatregelen die voortkomen uit de voorgaande stappen. Op het moment dat leveranciers inschrijven op de aanbesteding/offerte moeten alle **(wettelijke) eisen, wensen en voorwaarden** bekend zijn.
2. De servicenormen worden opgenomen in een **Service Level Agreement** (SLA). Een SLA is zeker bij SaaS-oplossingen noodzakelijk.
3. Opstellen van een (concept) **verwerkers-overeenkomst** met ondersteuning van de privacy coördinator.
4. Het is in grote aanbestedingen gebruikelijk alle onderkende eisen en wensen (dus ook die t.a.v. informatiebeveiliging, privacy en de archiefwet) te verzamelen in een **Programma van Eisen** (PvE).
5. Voorafgaand aan het inkooptraject wil Inkoop (via het **inkoop-startformulier**) o.a. weten wat er wordt aangekocht (een werk, levering of dienst), het type overeenkomst, de opdrachtwaarde, de contractduur en de geraamde kosten (indien bekend), de gunningscriteria met motivatie, welke aanbestedingsprocedure wordt gevolgd, en of er afgeweken wordt van de aanbevolen procedure en inkoopvoorwaarden. In dat laatste geval moet er ook een **afwijkadvies** worden opgesteld.

Toelichting - *We zijn verplicht leveranciers te selecteren op objectieve gronden, daarom moet elk inkooptraject beginnen met een welgekozen inkoopstrategie. Bij de aankoop van diensten en producten worden de algemene Inkoopvoorwaarden Drechtsteden gevolgd. Deze bevatten bepalingen betreffende de offerte, de opdracht, de uitvoering, de totstandkoming van de overeenkomst, de financiën, wettelijke kaders en vereisten, de leveringen van goederen en het verrichten van diensten. Het bevat ook bepalingen t.a.v. de opzegging, ontbinding en vernietiging van de overeenkomst.*

E. Realisatie / Implementatie

1. Richt de oplossing in, en implementeer deze (voor projecten) conform een eerder door de projectleider of projectverantwoordelijke opgesteld **projectplan**. Houdt hierbij rekening met de architectuur en alle geldende kaders en wet- en regelgeving (zie Deel 2).
2. Betrek vroegtijdig de lijn en de toekomstige beheerders van de oplossing, en regel de financiële consequenties op lange termijn (terugkerende beheerlasten staan los van de initiële projectkosten).

F. Overdracht naar de lijn en naar beheer

1. Betrek tijdens de realisatiefase technisch- en functioneel beheerders om de oplossing in productie en in beheer te krijgen. Regel het beheer op een structurele manier (ook financieel).
2. Maak zo nodig een **plan of draaiboek** voor de livegang, en zorg dat er aantoonbaar voldaan is aan alle eerder onderkende en gestelde bepalingen/eisen/richtlijnen.
3. Aandachtspunten voor livegang (voor zover van toepassing):
   - Communicatie verzorgen richting alle betrokkenen.
   - Kennisborging en opleidingen voor medewerkers.
   - Zorgen dat vragen van medewerkers beantwoordt kunnen worden en/of dat er een (telefonische) helpdesk beschikbaar is.
4. Ga na of de opdrachtgever kan **aantonen** dat de oplossing voldoet aan alle (wettelijke) vereisten en bepalingen uit alle voorgaande stappen, en dat aanbevelingen uit het privacy advies zijn opgevolgd. T.a.v. privacy en informatiebeveiliging is het nodig dat dit op schrift is vastgelegd (in goed overleg met de betrokken functionarissen).
5. Formele overdracht naar beheerders, met aanlevering van alle benodigde c.q. aanwezige informatie, waaronder:
   - productdocumentatie en systeem-handleidingen (indien aanwezig);
   - of een applicatie buiten ons eigen netwerk e-mails verzend namens de gemeente (mailrelay);
   - of automatisch inloggen nodig is (SSO - Single Sign On)?
   - of de Saas-criteria zijn nageleefd?
   - of de periodieke controle op de logging en autorisaties is geborgd/belegd?
   - of er een ondertekende verwerkersovereenkomst is?
   - of er systeemkoppelingen nodig zijn?
   - of er technische afhankelijkheden zijn met de bestaande IT-infrastructuur?
   - of de vernietiging van informatie goed is ingeregeld?
   - Ruim oude software en gegevens op (bij vervangingstrajecten) of migreer deze naar een andere oplossing. Team DIV kan hierbij adviseren.

iKaders Deel 2 - Richtlijnen en wettelijke vereisten (1/3)

	1. Informatiebeveiliging	2. Werken met persoonsgegevens	3. Data Protection Impact Assessment (DPIA)
Is deze situatie van toepassing?	Voor elke toepassing die gegevens verwerkt of vastlegt moet bepaald worden welke informatiebeveiligingsmaatregelen getroffen en onderhouden dienen te worden, om onze cyberweerbaarheid te waarborgen, en om datalekken en ongeoorloofde toegang tot gegevens te voorkomen.	Wordt in de applicatie of in het project met persoonsgegevens gewerkt? Zo ja, dan moet er altijd advies worden gevraagd aan de privacy coördinator. Breng de opdrachtgever op de hoogte dat advies is gevraagd. De aanbevelingen uit het advies dienen te worden opgevolgd, en maak aantoonbaar richting de opdrachtgever dat advies is gevraagd.	Is een van onderstaande criteria van toepassing? ▪ Evaluatie of scoretoekenning ▪ Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg ▪ Stelselmatige monitoring ▪ Gevoelige gegevens of gegevens van zeer persoonlijke aard ▪ Op grote schaal verwerkte gegevens ▪ Matching of samenvoeging van datasets ▪ Gegevens met betrekking tot kwetsbare betrokkenen ▪ Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen ▪ De situatie waarin als gevolg van de verwerking zelf "betrokkenen [...] een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst"
Zo ja, wat dan?	1. Bepaal de **dataclassificatie**. Het uitvoeren van een dataclassificatie is altijd verplicht. Het beschermingsniveau van gegevens (data) en/of informatiesystemen wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid. Mede aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke maatregelen moeten worden genomen. Voor het bepalen van de dataclassificatie wordt de handreiking van de informatie-beveiligingsdienst (IBD) als leidraad gehanteerd. 2. Voer daarna een **risicoanalyse** uit. De aanpak van onze informatieveiligheid is risico gebaseerd. Dat wil zeggen dat beveiligingsmaatregelen worden getroffen en onderhouden op basis de resultaten uit de dataclassificatie en het bepalen van het bijbehorende basisbeveiligingsniveau-toets (BBN). Vanaf BBN2 dient een aanvullende (diepgaande) risicoanalyse te worden uitgevoerd. Een lokale adviseur informatiebeveiliging kan je met deze zaken ondersteunen en adviseren. Vraag de leverancier altijd om alle relevante documentatie, en in ieder geval naar de aanwezigheid van deze stukken: ▪ actueel **ISO 27001 certificaat**, inc. verklaring van toepasselijkheid; ▪ rapportage van de meest actuele **pentest** (een penetratietest of pentest is een toets van computersystemen op kwetsbaarheden); ▪ een **ISAE 3000 soc2 assurance** verklaring met daarin de trust service principes of een soortgelijke (TPM) verklaring. Bij de beoordeling van andersoortige stukken wordt o.a. gelet op: backups, updates en patches, cryptografische beheersmaatregelen, beveiligde inlogprocedure, fysieke toegangsbeveiliging, security awareness, training, logging en monitoring van gebruikersacties, veilig uitwisselen van informatie en certificeringen. **De Radio Equipment Directive** bevat in artikel 3 (RED 3.3) cybersecurity eisen voor fabrikanten en importeurs die betrekking hebben op radioapparatuur (en daarmee van toepassing op mobiele devices, Internet of Things (IoT), sensors, drones, communicatie- en betalingsystemen).	Uit het advies van de privacy coördinator blijkt welke van deze documenten moeten worden opgesteld: ▪ Een **verwerkersovereenkomst** (naar modelovereenkomst van de VNG); ▪ Indien nodig een **privacyverklaring**; ▪ indien nodig een **privacyscan;** ▪ indien nodig een **DPIA (Data Protection Impact Assessment)**, ▪ Indien nodig een **cookieverklaring**; ▪ Indien nodig een **juridische toets** door JKC (via Weten en Regel op SID); ▪ Indien nodig een **risicoacceptatie-formulier** voor het accepteren van rest-risico's. Invullen i.s.m. de proceseigenaar. Als gemeente hebben we de verplichting om een register van gegevensverwerkingen bij te houden. Alle gegevensverwerkingen worden opgenomen in het **verwerkingsregister**. In dit register staat het doel van de verwerking, om wat voor soort gegevens het gaat, wie er toegang toe hebben, of gegevens aan andere partijen of applicaties worden doorgegeven, en hoe lang de gegevens worden bewaard. Belangrijk om te weten: ▪ Het nemen van privacy-maatregelen zijn integraal onderdeel van de informatieverwerking; het waarborgt het privacybeleid gedurende de hele levenscyclus van persoonsgegevens. ▪ We mogen persoonsgegevens alleen verwerken voor een vooraf duidelijk bepaald doel en mogen die gegevens niet zonder meer verder verwerken voor andere doeleinden. ▪ We leggen alleen die data vast die noodzakelijk is voor het gebruiksdoel (dataminimalisatie), en alleen voor zolang nodig of wettelijk verplicht. ▪ De toegang tot gegevens en functionaliteit voor medewerkers en burgers is afgestemd op hun rol en functie. ▪ Betrokken burgers hebben het recht om gegevens in te zien, te wijzigen, te laten verwijderen, over te dragen, en het recht om vergeten te worden. Processen en applicaties moeten hierop zijn ingericht.	Zeer waarschijnlijk moet er – conform artikel 35 van de Algemene Verordening Gegevensbescherming – een **Data Protection Impact Assessment (DPIA)** worden opgesteld. Dit een verplichting die geldt voor projecten, regelgeving en beleid. Deze verplichting vloeit voort uit de Algemene Verordening Gegevensbescherming (AVG). Het is een onderzoek dat duidelijk maakt of en waar grote privacyrisico's ontstaan als je persoonsgegevens gebruikt. ▪ Betrek een privacy coördinator; hij of zij ondersteunt je bij het uitvoeren van de DPIA en toetst en adviseert samen met een lokale adviseur informatiebeveiliging over aanvullende systeemeisen en maatregelen. ▪ Leg de DPIA ter advisering voor aan de functionaris gegevensbescherming (FG) van de Drechtsteden. Eventueel kunnen er aanpassingen nodig zijn. Daarna kan de DPIA ter vaststelling worden voorgelegd aan de betreffende manager. ▪ Belangrijk: je mag wettelijk niet met een nieuwe gegevensverwerking waarvoor een DPIA verplicht is beginnen, als de DPIA nog niet is afgerond en er nog geen advies van de FG ligt!

Het beantwoorden van de vragen uit het **'Toetsingsdocument Applicaties - Informatiebeveiliging & Privacy'** wordt geadviseerd door de functionaris gegevensbescherming (FG) van de Drechtsteden bij de beoordeling van **(nieuwe) applicaties en systemen**. Bespreek het resultaat zowel met de privacy coördinator als met de Informatie Security Officer. Veel van het bovenstaande komt ook in dit document ter sprake.

iKaders Deel 2 - Richtlijnen en wettelijke vereisten (2/3)

	4. Archiveren	5. Nieuwe software	6. Uitwisselen van gegevens	7. BI en rapportages	8. Technologische bepalingen:
Is deze situatie van toepassing?	Wordt in de applicatie met een van onderstaande gegevens gewerkt? ▪ een formeel contact of correspondentie met een burger, bedrijf of ketenpartner; ▪ een formeel (intern) verzoek, advies of besluit(vorming); ▪ een bindende afspraak (zoals een beschikking, vergunning, besluit, contract of overeenkomst). ▪ een website met informatie aangaande een publieke taak van de gemeentelijke organisatie.	Een informatiearchitect geeft inzicht in de mogelijkheden van reeds aanwezige c.q. eerder aangeschafte software. Is er toch nieuwe software nodig?	Is er sprake van uitwisseling van gegevens tussen applicaties of databronnen onderling?	Worden gegevens overgezet naar een centrale (dataware-house) omgeving waarin gegevens uit meerdere applicaties of databronnen samen komen, met de bedoeling om er (management-) rapportages, dataanalyses of (geo)visualisaties van te maken?	**8a.** Is de applicatie een **Saas-applicatie**? Laat de leverancier de antwoorden op de eisen uit (de laatste versie) van het document "**ICT beleid – Technische SaaS applicatiecriteria versie 11**" invullen. Met dit document worden de eisen ten aanzien van de techniek van de SaaS applicatie getoetst. Laat de uitkomsten toetsen door een technisch architect. Deel de uitkomsten ook met de Informatie Security Officer. **8b.** Is **een app op een telefoon of tablet** onderdeel van de oplossing? Laat de leverancier dan het document "**ICT beleid – mobiele apps criteria**" invullen. Met dit document worden de eisen die gesteld worden aan apps op mobiele devices getoetst. Laat de uitkomsten toetsen door een technisch architect en deel de uitkomsten ook met de Informatie Security Officer. **8c.** Is **ondersteuning op afstand** nodig waarbij een PC of laptop overgenomen wordt? Er is beleid opgesteld voor externe toegang en beheer op afstand. Betrek een technisch architect en een Informatie Security Officer.
Zo ja, wat dan?	De **Archiefwet** is van toepassing. De informatie moet gedurende de wettelijke bewaartermijn juist en volledig worden opgeslagen en na afloop van de bewaartermijn vernietigd worden of na 20 jaar overgebracht worden naar het Regionaal Archief Dordrecht. Betrek Team Digitale Informatievoorziening c.q. DIV. Zij toetsen en adviseren over aanvullende systeemeisen aan de hand van een **informatieanalyse**. Hierin wordt uiteengezet wat, hoe en waar gearchiveerd kan worden. In de inventarisatiefase kijkt DIV o.a. naar de werkprocessen, informatie(objecten), kanalen, bewaartermijn(en) en i.v.t. website. Dit bepaalt de aanvullende eisen (Archiefwet) voor aankoop. In de implementatiefase is het o.a. belangrijk dat de informatie (objecten) goed geordend worden, de bewaartermijnen zijn ingericht en het (jaarlijkse) vernietigings-proces is afgestemd met Team DIV en de archiefinspecteur. Twijfelt je wat te doen met de informatie in de oude oplossing? Neem dan ook contact op met Team DIV. Informatie mag enkel vernietigd worden na akkoord van de archiefinspecteur. Voor migratie van gegevens dient een **migratie-plan** te worden geschreven.	Te volgen richtlijnen: • Data dient te worden opgeslagen binnen de EU. • Hergebruik van bestaande software gaat voor kopen, en kopen gaat voor bouwen. Als er reeds een goede applicatie beschikbaar is binnen de Drechtsteden, dan wordt deze breder ingezet. En denk daarbij ook aan de mogelijkheden van Microsoft 365 (M365). • Bij het kopen van software hanteren we een SaaS-tenzij beleid. Daarmee wordt bedoeld dat we software willen die online als dienst of service wordt aangeboden. In principe hosten we software niet zelf; als dat wel het geval is gelden de **aansluit-voorwaarden van KPN**. • We zijn zeer terughoudend met het (laten) bouwen van maatwerk. Maatwerk is zowel in realisatie maar vooral ook in onderhoud duur en zeer tijdsintensief. Het op maat configureren van standaardcomponenten (bijvoorbeeld in M365) is wel mogelijk. • Waar mogelijk gebruiken we softwarecomponenten en -services die langs de lijnen van Common Ground (CG) zijn ont-wikkeld. CG is de landelijke i-visie van VNG voor gemeenten. • Voor nieuwe SaaS-applicaties is Single Sign On en authenticatie via Entra ID vanuit beveiligings-oogpunt verplicht gesteld conform het pas-toe-of-leg-uit principe. Bespreek afwijkingen met de Chief Informatie Security Officer (CISO).	Betrek een informatiearchitect om met je mee te denken en eventueel e.e.a. in beeld te brengen in een **architectuurschets**. Betrek je lokale adviseur informatiebeveiliging omwille van de beveiliging van het transport, en een privacy coördinator wanneer het persoonsgegevens betreft. Uitgangspunten bij systeemkoppelingen: ▪ Ga na of de gegevensuitwisseling is toegestaan. ▪ Waak ervoor dat dezelfde gegevens niet op verschillende plekken worden vastgelegd en onderhouden. ▪ Voor gegevens die in een landelijke basisregistratie beschikbaar zijn, geldt de verplichting deze uit de basisregistratie te betrekken. Waar mogelijk sluiten we aan op de landelijke Haal Centraal API's. ▪ Betrek gegevens uit de gezaghebbende bron (d.w.z. een kernregistratie of daar waar 'de waarheid' wordt beheerd en onderhouden). ▪ Een applicatie die het proces ondersteunt, de bronapplicatie, is verplicht haar authentieke gegevens met andere applicaties te delen, wanneer deze gegevens uit de bron nodig heeft. ▪ De techniek om gegevens uit te wisselen is in de hele keten zoveel als mogelijk gestandaardiseerd. Momenteel is deze standaard: API's. Bij het vervangingen en upgraden van koppelingen zijn moderne API's het uitgangspunt. ▪ Wanneer een bron meerdere afnemers heeft, wordt bekeken of de aansluiting via een centrale voorziening kan worden opgezet zodat de verbinding maar één keer gerealiseerd hoeft te worden. Op deze manier is het ook mogelijk om logging, technisch beheer en certificaten-beheer eenmalig in te regelen. ▪ Informatie die we delen vanuit de door ons beheerde bronnen, moet ook bij de afnemer voldoen aan de door ons gestelde eisen voor privacy en beveiliging. De eisen op de bron gelden dus ook voor afnemers. Structurele leveringen van gegevens, en ook ad hoc leveringen van persoons-gegevens, worden vastgelegd in een **gegevensleverings-overeenkomst (GLO)**. Hierin komen ook onderwerpen als doelbinding en (wettelijke) grondslag aan bod.	Betrek de Chief Data Officer (CDO) om met je mee te denken en te adviseren. De volgende uitgangspunten worden gehanteerd: ▪ Gegevens die voor deze doeleinden benodigd zijn, worden centraal en onafhankelijk van een specifieke rapportage- of visualisatie-tool ter beschikking gesteld. ▪ Rapportages en visualisaties waarin gegevens uit meerdere eigen bronnen samenkomen, komen via een door de organisatie centraal aangewezen platform tot stand. ▪ Gebruik van en toegang tot gegevens vindt plaats binnen wettelijke kaders.	

iKaders Deel 2 - Richtlijnen en wettelijke vereisten (3/3)

	9. Dienstverlening	10. AI en algoritmes	
Is deze situatie van toepassing?	Wordt er (digitale) dienstverlening gerealiseerd?	Wordt er gebruik gemaakt van AI-technologie of van algoritmes?	
Zo ja, wat dan?	Benader de dienstverlening zo integraal mogelijk, georganiseerd vanuit het perspectief van burgers en ondernemers. Kernwoorden daarbij zijn: duidelijk hoe af te nemen, efficiënt, gebruikers-vriendelijk, begrijpelijk, voorspelbaar, toegankelijk, begrijpelijke taal, in 1 keer goed geholpen. **M.b.t. de Wet modernisering elektronisch bestuurlijk verkeer (Wmebv)**: via deze wet krijgen inwoners en ondernemers het recht om officiële berichten elektronisch aan gemeenten en andere overheidsorganisaties te versturen. Het gaat om berichten die bijvoorbeeld gaan over een aanvraag, melding, beschikking, besluit, klacht, bezwaar of beroep. Dit verloopt via een digitaal kanaal, en bij voorkeur via een webformulier. Bij de aanschaf van nieuwe applicaties gelden de volgende functionele vereisten: • logging van berichten; • t.a.v. het digitaal ontvangen van berichten: *1)* verzenden van een ontvangstbevestiging, *2)* gegevens terug kunnen tonen, *3)* webformulier met data-minimalisatie en zonder belemmeringen in gebruik; • t.a.v. het verzenden van berichten komen er later aanvullende kaders.	Betrek de Chief Data Officer (CDO). Algoritmen worden in de toekomst vastgelegd in het **landelijke algoritme-register**. AI-toepassingen moeten in gebruik en ontwikkeling voldoen aan de Europese AI-verordening. Voorwaarden zijn vastgelegd in een "**Gids AI-verordening**" *https://www.rijksoverheid.nl/documenten/brochures/2024/10/16/gids-ai-verordening*	

Aanvullingen op de iKaders inzake DG&J

Informatiebeveiliging
- Bepaal de dataclassificatie en voer de risicoanalyse uit op basis van BIV en het Strategisch Informatiebeveiligings-beleid van DG&J.
- Vraag leveranciers om alle relevante documentatie, en in ieder geval naar de aanwezigheid van deze stukken:
  - actueel NEN 7510 certificaat inclusief Verklaring van Toepasselijkheid (VvT)
  - voeg expliciet eisen toe op basis van NEN 7510. Gebruik de "NEN 7510 eisenlijst voor leveranciers" als bijlage (zie Qlink)
  - Vraag leveranciers of ze NEN 7510-audits ondergaan

Werken met persoonsgegevens
Verwerk in de verwerkersovereenkomst of SLA:
- naleving van NEN 7510;
- meldplicht datalekken;
- logging & monitoring-verantwoordelijkheden;
- toegang op basis van behandelrelatie ((indien van toepassing);
- bewaartermijnen en vernietigingsbeleid volgens AVG én medische bewaarplicht.

Eisen aan Saas-oplossingen
In de iKaders wordt onder 8b verwezen naar de "Technische SaaS applicatiecriteria". Breid deze toets uit met NEN 7510-aspecten, zoals:
- scheiding van data per klant (multi-tenant model),
- back-upprocedures binnen EU,
- versleuteling van medische gegevens in rust en in transport,
- beveiliging van beheerdersinterfaces,
- rol gebaseerde toegang.

Logging & autorisatiebeheer
Ga al bij de selectie van de applicatie na of deze:
- auditbare logging ondersteunt op gebruikersniveau;
- voorzien is van controleerbare autorisatiemodellen;
- mogelijkheden heeft voor controle van toegang op behandelrelatie (NEN 7510-specifiek).

Privacy en DPIA vóór aankoop gereed!
- Betrek de Functionaris Gegevensbescherming (FG);
- Voeg de uitkomsten toe aan de besluitvorming;
- Koppel de resultaten terug naar de leverancier met eisen voor inrichting (bijv. pseudonimisering, logging, dataminimalisatie).

Interoperabiliteit en beveiliging van koppelingen
Let bij koppelingen met andere applicaties of landelijke voorzieningen (zoals LSP of KIK-V) op:
- Of de technische- en beveiligingsarchitectuur hierop is voorbereid;
- Laat een informatiearchitect én ISO toetsen op standaarden, logging, beveiligde transportprotocollen (API's, TLS, etc.).

Plan voor bewustwording en beheerorganisatie
Het implementatieplan moet ook bevatten:
- Trainingen voor gebruikers en beheerders over privacy en beveiliging (conform NEN 7510);
- Afspraken over wie wat monitort: bijv. wie bekijkt de logs en hoe vaak?