Algemeen informatiebeleid

Provincie Zeeland
2021-2024

Provincie Zeeland

Algemeen informatiebeleid

Provincie Zeeland
2021-2024

Datum	16 februari 2021
Auteur	Afdeling IA
Versienummer	1.0

Inhoudsopgave

1. Inleiding

Informatiebeleid is een fundament om professioneel te kunnen werken in de context van een overheidsorganisatie. Informatie is namelijk een essentiële grondstof voor alle processen, van uitvoering tot bestuurlijke besluitvorming. Iedere medewerker en bestuurder maakt hier op allerlei manieren dagelijks gebruik van.
Door te werken volgens de gedachten vanuit het informatiebeleid verzekeren we onszelf van belangrijke voordelen, om er een aantal te noemen: informatiesystemen die aansluiten op de inrichting van een bedrijfsproces en zelfs hogere strategie, eenvoudige uitwisseling van data met andere partijen, adequate ondersteuning door middel van duidelijke beheerrollen, beslissingen die worden genomen op basis van betrouwbare informatie, geoorloofd gebruik van gevoelige data enz.
De risico's van het niet hanteren of niet naleven van informatiebeleid laten zich eenvoudig raden: slecht werkende informatiesystemen, leveranciers die niet aan afspraken gehouden kunnen worden, samenwerking bemoeilijkt omdat data niet uitgewisseld kan worden, risico's in de bedrijfscontinuïteit en zelfs risico's informatieveiligheid en privacy.
Met zorg is gewerkt aan een integraal informatiebeleid dat past bij onze organisatie en meegroeit op de ontwikkelingen. Ontwikkelingen die niet enkel binnen onze organisatie plaatsvinden maar natuurlijk ook landelijk en internationaal.

In het voorgaande Informatiebeleid Provincie Zeeland is er voor gekozen om het beleid op hoofdlijnen te houden waarbij met name de verantwoordelijkheden beschreven zijn.
Bij het opstellen van dit Algemeen Informatiebeleid is gekozen om deze lijn door te zetten. Hierbij is geanticipeerd op de ontwikkelingen van de afgelopen jaren. Denk daarbij aan:

- Veranderende scope van Provincie Zeeland
  In de afgelopen jaren krijgt de digitalisering een steeds sterkere rol. Het omgaan met informatie en gegevens speelt een steeds grotere rol in ons werk (dataficering). De scope van Provincie Zeeland gaat daarbij meer en meer naar buiten. Samenwerking aan maatschappelijke opgaves staat centraal. Op steeds meer beleidsvelden ontstaan samenwerkingsconstructies die behoefte hebben om zichzelf te profileren, informatie te delen en deze te ontsluiten. Samenwerkingsvormen kunnen telkens variëren: we willen kunnen schakelen in die variatie. Provincie Zeeland kan daarbij verschillende rollen spelen en is soms initiatiefnemer, opdrachtgever maar kan ook deelnemer of financier (subsidie) zijn. Binnen welke kaders oplossingen worden ontwikkeld is niet altijd even helder. Hierop willen we vanuit en via het informatiebeleid op anticiperen. Uiteindelijk zien we dat bij alle maatschappelijke opgaves informatievraagstukken en digitalisering een rol spelen. Provincie Zeeland heeft inmiddels een verkenning uitgevoerd naar een Digitale Agenda Zeeland.

- Doorontwikkeling informatiehuishouding
  De doorontwikkeling van de eigen informatievoorziening gaat ook onverminderd voort, en zal de komende jaren steeds meer externe componenten bevatten. Steeds meer oplossingen worden als een service in de cloud beschikbaar gesteld. Daarmee wordt het informatielandschap complexer en wordt regie belangrijker. De Corona-crisis geeft dit proces een versnelling.
  We willen weten wat er in Zeeland speelt, vanuit de rollen die de Provincie in de Zeeuwse

maatschappij speelt. We willen gefundeerde keuzes maken en beslissingen nemen. We willen zien wat het effect van onze beslissingen is en daar, indien gewenst, op bij sturen. Informatievoorziening heeft een zichtbare bijdrage aan de Zeeuwse opgaven en programma's en bijbehorende reguliere taken. We willen daarvoor over goede en tijdige informatie kunnen beschikken. Data geven de basis voor de kwaliteit van de informatie.
We willen een vertrouwde partner zijn: voor inwoners, bezoekers en bedrijven; voor collega-overheden (provinciaal, nationaal en internationaal). We willen *in control* zijn bij de diverse rollen die we in het informatienetwerk spelen.
We willen informatie en data een actieve rol in onze bedrijfsprocessen laten spelen. Digitalisering heeft een bepalende invloed op de (ontwikkeling van de) inrichting van onze processen. Sturen we hier niet op, dan hebben we onvoldoende grip op hoe onze processen uitgevoerd worden. Denk aan managementinformatie, Business Intelligence, IoT, kunstmatige intelligentie, robotisering etc. We willen onze informatie (en onderliggende data) op een ethisch en juridisch verantwoorde, beschermde en beveiligde wijze vergaren en gebruiken. We weten wat we doen, we zijn ons daar bewust van en we kunnen dat goed aan onze stakeholders en opdrachtgevers uitleggen. We zijn goed in staat om onze democratische verantwoording daarover af te kunnen leggen. Daarvoor willen we ook dat we aansluiten bij (internationale) digitaliseringsontwikkelingen, (open) standaarden en technieken. Anders zijn we onvoldoende verbonden in het informatienetwerk. Dit is een bewegend doel: immers, digitalisering blijft zich ontwikkelen, blijft veranderen en dat alles in een steeds hoger tempo.

- Digitalisering als gevolg van wet- en regelgeving
  Wet- en regelgeving ontwikkelt zich door en heeft een steeds grotere impact op digitalisering. Denk daarbij aan: de Wet Open Overheid, de Omgevingswet, de Wet Elektronische Publicaties, de nieuwe Archiefwet, de Wet Digitale Overheid, de Wet en regelgeving Basisregistraties, de Algemene Verordening Gegevensbescherming, de Dienstenwet en het Tijdelijk Besluit Digitale Toegankelijkheid overheid.

- Beveiliging en privacy
  Gedeputeerde Staten hebben in 2018 besloten dat Provincie Zeeland toewerkt naar een ISO 27001-certificering op het gebied van informatieveiligheid. In het kader van de implementatie van deze ISO-norm is eind 2019 apart deelbeleid voor informatieveiligheid vastgesteld.
  Met het oog op de verdere implementatie van de Algemene Verordening Gegevensbescherming (AVG) is apart deelbeleid voor privacy vastgesteld (privacybeleid en privacyreglementen).

2. Context van het Algemeen Informatiebeleid

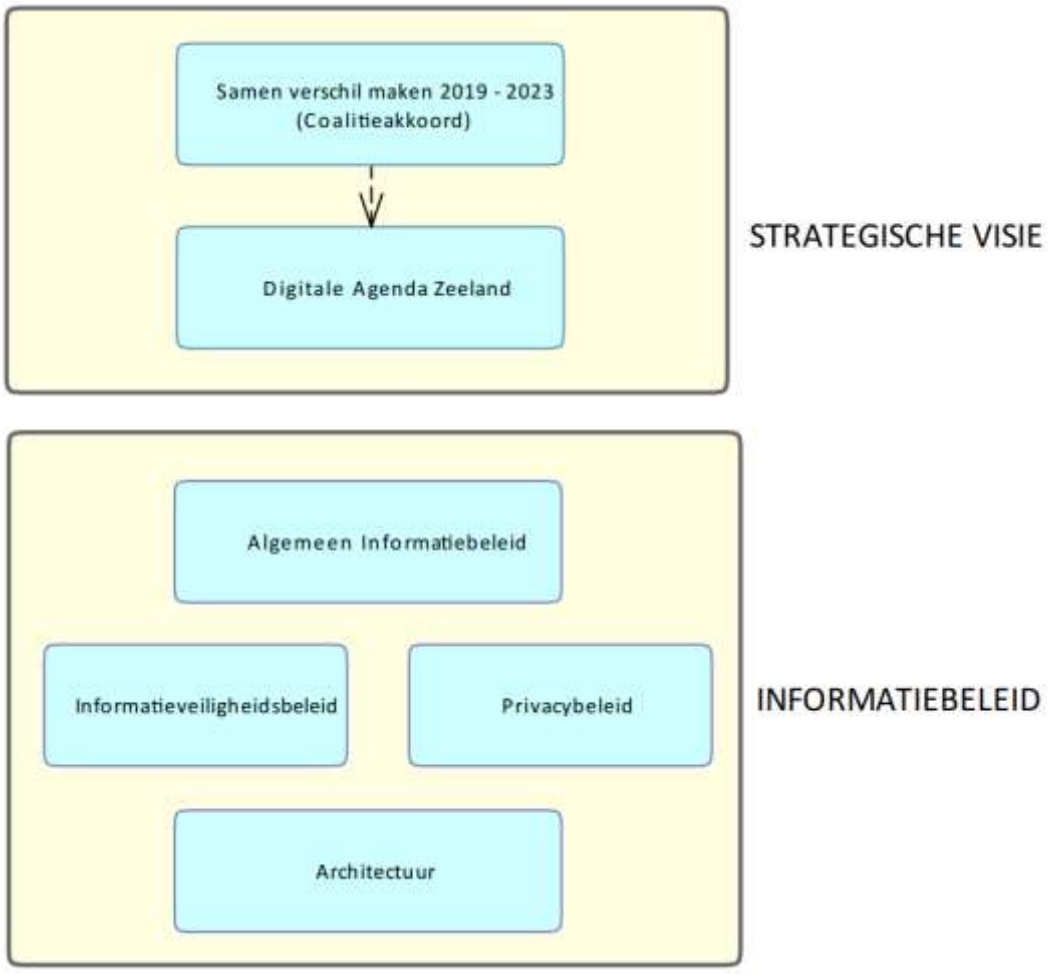
Strategische Visie

Tot op heden ontbreekt een provinciale strategische visie op de maatschappelijke digitaliseringsvraagstukken. Vanuit het Rijk is medio 2018 een overheidsbrede visie neergezet (NL DIGIbeter), en ook interprovinciaal wordt er gewerkt aan een Interprovinciale Digitale Agenda (IDA 2.0). Deze IDA kent 4 sporen, te weten: Bedrijfsvoering, Dienstverlening, Innovatie, en Data. Naar aanleiding van het coalitieakkoord Samen Verschil maken 2019-2023 is deze strategische visie nu in ontwikkeling (Digitale Agenda Zeeland). Er is inmiddels een verkenning uitgevoerd, en daarmee is in dit Algemeen Informatiebeleid rekening gehouden.

Informatiebeleid

De afgelopen jaren is er apart deelbeleid ontwikkeld voor Informatieveiligheid en Privacy. Voor de meer algemene informatiebeleidsaspecten is daarom dit Algemeen Informatiebeleid opgesteld. Het Informatiebeleid (totaal) wordt gevormd door het Algemeen Informatiebeleid (dit document), het Informatieveiligheidsbeleid, het Privacybeleid en de onderliggende Architectuur. Deze beleidsdocumenten zijn op elkaar afgestemd en zijn vooralsnog onafhankelijk van de inhoud van de Strategische Visie.

Hieronder is op hoofdlijnen weergegeven wat de context is van het Algemeen Informatiebeleid in het geheel:



In bijlage 2 is dit schema verder in detail uitgewerkt

3. Doelen van het Algemeen Informatiebeleid

Zoals in hoofdstuk 2 is aangegeven bestaat het informatiebeleid uit meerdere componenten die samen de kaders en richtlijnen bepalen die we hanteren bij nieuwe ontwikkelingen. Het Algemeen Informatiebeleid is gericht op het realiseren van de volgende doelen:

- De organisatie wil snel kunnen anticiperen op (digitale) ontwikkelingen,
- De informatievoorziening is optimaal afgestemd op de doelstellingen van de organisatie
- De organisatie moet de spelregels kennen en toepassen als er informatievraagstukken spelen, dit geldt zowel intern als in samenwerkingsverbanden. Bij samenwerkingsverbanden is de rol die de Provincie Zeeland heeft van invloed op de te hanteren spelregels.

4. Uitgangspunten van het Algemeen Informatiebeleid

Met betrekking tot de toepassing van het Algemeen Informatiebeleid worden de volgende uitgangspunten gehanteerd:

1. Ontwikkelingen waarbij verandering nodig is ten aanzien van informatievoorziening worden getoetst aan de architectuur, het informatieveiligheidsbeleid en de privacywetgeving. Dit om ervoor te zorgen dat alle relevante aspecten op een juiste wijze in de uitwerking worden meegenomen en blijvend worden geborgd.
   De digitalisering zet steeds verder door en vrijwel alle ontwikkelingen in de organisatie hebben een informatieaspect. Niet in alle gevallen wordt dit als zodanig herkend. Het is essentieel dat medewerkers bewust met informatie omgaan. Indien er nieuwe ontwikkelingen worden geïnitieerd dient de afdeling IA in een zo vroeg mogelijk stadium te worden betrokken, zodat ook pro-actief kan worden meegedacht.
   De medewerkers worden hierover bewust gemaakt en geïnformeerd, o.a. middels het organiseren van interne trainingen en/of workshops. Hiervoor is ondersteuning vanuit de afdeling IA i.s.m. POJZ beschikbaar.

2. Indien bij een ontwikkeling wordt afgeweken van het Informatiebeleid moet dit expliciet worden gemotiveerd. Dit wordt vastgelegd in een zgn. waiver[1]. Uitgangspunt daarbij is dat de betreffende ontwikkeling is afgestemd met de provinciale architecten en indien relevant ook de CISO en/of de Senior Jurist Privacy. Bij afwijking hiervan wordt, afhankelijk van de omvang van de bedrijfsrisico's, besloten of de voorgenomen invulling ter besluitvorming wordt aangeboden aan het college van Gedeputeerde Staten.
   Het Algemeen Informatiebeleid, het Informatieveiligheidsbeleid, het Privacybeleid en de Architectuur zijn leidend bij verandervraagstukken met een informatiecomponent. De provinciale architecten, de Chief Information Security Officer (CISO), Data Officer, Senior Jurist Privacy en de Functionaris Gegevensbescherming (FG) bewaken de bijbehorende kaders en dienen dus bij dergelijke veranderingen betrokken te worden en te beoordelen of een gewenste oplossing aansluit bij de kaders. Als blijkt dat een gewenste oplossing niet past binnen de kaders van het informatiebeleid, dan mag alleen gemotiveerd worden afgeweken en wordt dit vastgelegd in een zgn. waiver. Als sprake is van een afwijking met significante bedrijfsrisico's wordt dit bovendien afgestemd met de eerder genoemde functionarissen en moet de CIO (Chief Information Officer) een positief advies geven. Vervolgens wordt de afwijking door de initiatiefnemer ter besluitvorming voorgelegd aan de directie.

3. Elke manager is binnen zijn/haar organisatieonderdeel (afdeling, team/unit, opgave, project of programma) verantwoordelijk voor de kwaliteit van de eigen informatiehuishouding en is zich hiervan bewust.
   De verantwoordelijkheid voor een adequate informatiehuishouding ligt bij afdelingen, team/unit, project, opgaven en programma's. Elke manager is daarbij zelf verantwoordelijk voor het actueel en betrouwbaar zijn van de door hen gegenereerde en beheerde informatie en neemt verbeteracties op in de jaarplannen. De afdeling IA stelt kaders, is verantwoordelijk voor het faciliteren van de digitale voorzieningen en adviseert over het actueel en betrouwbaar houden van de informatie. Hierbij wordt het eigenaarschap van informatie duidelijk in de organisatie belegd. Daarnaast moeten medewerkers met de verdergaande digitalisering meer informatiebewust worden. Leidinggevenden dienen hier op te sturen. De benodigde acties worden vastgelegd in het jaarplan van de betreffende afdeling, de opgave of het programma.
   Voor elke applicatie (incl. inrichting), dataset en voor elk proces is op managementniveau een eigenaar benoemd die verantwoordelijk is voor de kwaliteit en de actualiteit. Elke eigenaar laat periodiek afhankelijk van het risicoprofiel aantoonbaar een toets uitvoeren op actualiteit van zijn eigen informatiehuishouding en of nog wordt voldaan aan actuele eisen t.a.v. architectuur, informatieveiligheid en privacy. Voor de verdere uitwerking van het eigenaarschap wordt verwezen naar "Bijlage 3 Eigenaarschap van processen, middelen en informatie".

[1] In een waiver wordt formeel vastgelegd voor welke termijn en onder welke voorwaarden het niet voldoen wordt toegestaan.

4. Gedeputeerde Staten zijn verantwoordelijk voor het actueel houden van het Algemeen Informatiebeleid en stelt minimaal één keer per vier jaar een nieuwe versie vast.
Voor het Algemeen Informatiebeleid wordt de bestuurlijke cyclus van vier jaar gevolgd.

5. De CIO is verantwoordelijk voor het actueel houden van de onderliggende kaders en richtlijnen en de Architectuur, waarbij ook landelijke kaders meegenomen worden, en stelt minimaal één keer per jaar een nieuwe versie vast.
Op basis van het Algemeen Informatiebeleid zijn kaders en richtlijnen uitgewerkt en vastgesteld. Deze worden periodiek geactualiseerd. De afdeling IA zorgt ervoor dat de Architectuur actueel blijft en deze wordt gebruikt om het Informatiebeleid te toetsen. De CIO is daarbij eindverantwoordelijk.

6. De afdeling IA faciliteert de informatievoorziening voor de gehele organisatie.
De afdeling IA faciliteert de basisvoorzieningen voor de gehele organisatie, zoals kantoorautomatisering, kernapplicaties[2], GEO functionaliteit, data-infrastructuur en basisregistraties. Voor de basisvoorzieningen worden infrastructuur, applicaties, licenties, devices en budgetten beheerd en actueel gehouden.

7. De afdeling IA bewaakt de toepassing van de provinciale architectuur en ondersteunt de organisatie bij het toetsen van nieuwe ontwikkelingen en het implementeren van nieuwe toepassingen.
Om goede invulling te kunnen geven aan artikelen één tot en met zes bewaakt de afdeling IA de toepassing van het informatiebeleid en biedt de afdeling ondersteuning bij het toetsen van ontwikkelingen. Er vindt vanuit de architecten coördinatie plaats op het effectief en efficiënt inrichten van het organisatiebrede applicatielandschap.
Voor het adviseren en toetsen van nieuwe ontwikkelingen wordt een vastgesteld proces gevolgd. Verder is er een aantal toetsingsinstrumenten beschikbaar. Het is van groot belang dat naast afdeling IA, ook adviseurs op het gebied van inkoop, juridische aspecten (privacy/contracten), financiën en communicatie in een zo vroeg mogelijk stadium worden betrokken. Zie bijlage 1 voor de schematische weergave. De in het schema genoemde functionarissen zorgen ervoor dat de juiste adviseurs vanuit andere disciplines tijdig betrokken worden in het proces. Het is belangrijk dat alle medewerkers worden geïnformeerd over deze aanpak en dat ze bewust worden gemaakt van het belang hiervan.

8. De CIO rapporteert jaarlijks aan het college van Gedeputeerde Staten omtrent de uitvoering van het informatiebeleid.
De verdergaande digitalisering van de organisatie betekent dat de informatiehuishouding de komende jaren volop aan verandering onderhevig is. In het coalitieakkoord is benoemd dat digitalisering de maatschappij op alle fronten doortrekt en daarmee ook de provinciale organisatie volop raakt. Het ontwikkelen van de Digitale Agenda Zeeland is benoemd. Belangrijk is dat de daarmee samenhangende acties worden uitgevoerd conform de uitgangspunten van het informatiebeleid. Met het oog daarop zal het college van Gedeputeerde Staten jaarlijks van de voortgang op de hoogte worden gehouden.

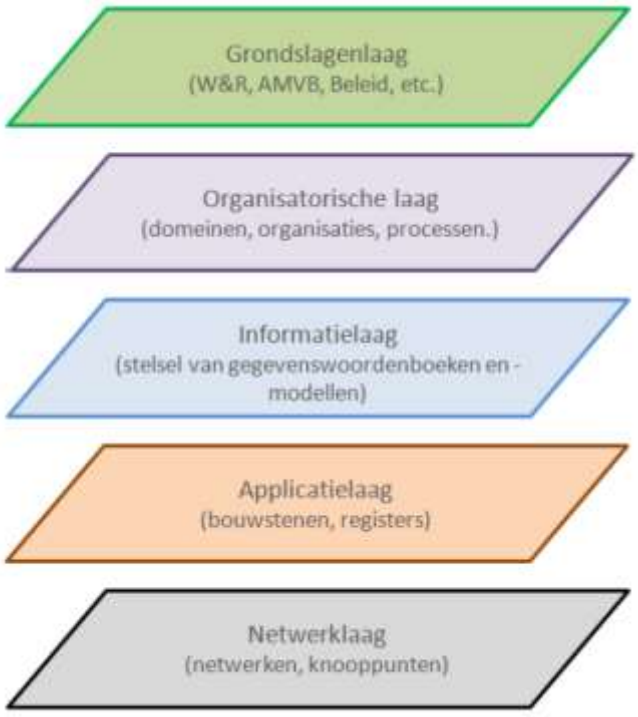
[2] Dit betreft generieke applicaties die provinciebreed worden gebruikt, bijvoorbeeld zaaksysteem, financieel systeem, inkoopsysteem

5. Toetsing ontwikkelingen

Nieuwe ontwikkelingen worden getoetst op de volgende aspecten:

- *Is de inhoudelijke en functionele vraag voldoende helder?*
- *Sluit de ontwikkeling aan op de bestuurlijke visie en de organisatievisie?*
- *Is er al een oplossing in gebruik?*
- *Is samenwerking voor de oplossing een reële optie: regionaal, provinciaal en/of overheidsbreed?*
- *Wordt de oplossing efficiënt en effectief ingevuld en past het binnen de Enterprise Architectuur (zie hoofdstuk 6)?*
- *Worden geldende open standaarden gehanteerd en is de uitwisselbaarheid geregeld?*
- *Wordt de beschikbaarheid, bruikbaarheid en bestendigheid van de data binnen de oplossing voldoende geborgd?*
- *Is eigenaarschap en verantwoordelijkheid van de verschillende aspecten van de oplossing geregeld?*
- *Is de beschikbaarheid en continuïteit van de oplossing geregeld?*
- *Zijn het beheer, de kennis en de capaciteit van de oplossing geregeld?*
- *Dient de informatie binnen de oplossing duurzaam te worden gearchiveerd?*
- *Voldoet de oplossing aan wet- en regelgeving?*
- *Voldoet de oplossing aan de kaders van informatieveiligheid?*
- *Voldoet de oplossing aan de kaders van het privacybeleid en de privacywetgeving?*
- *Zijn er bij de oplossing ethische aspecten aan de orde?*
- *Zijn de benodigde financiële middelen, de juridische toetsing en/of de licenties voor de oplossing geregeld?*
- *Wordt met de oplossing voldaan aan de kaders van het inkoop- en aanbestedingsbeleid?*

Deze aspecten worden in relatie gebracht met de effecten op de volgende lagen vanuit de architectuur Provincie Zeeland (gebaseerd op het 5 lagen model van de Nederlandse Overheids Referentie Architectuur NORA):



6. Uitgangspunten Onderliggende Architectuur

In de onderliggende Enterprise Architectuur worden onderstaande uitgangspunten gehanteerd[3].

1. We streven naar samenwerking met andere partijen.
   We streven naar samenwerking met andere overheden, centrale oplossingen in beheer bij IPO en aansluiting op landelijke bouwstenen. Hiermee bevorderen we hergebruik en veilige informatie-uitwisseling tussen overheden. Gezamenlijk door Provincies ontwikkelde bouwstenen worden ondergebracht bij een gemeenschappelijke beheerorganisatie. Gemeenschappelijk gebruik leidt tot kostenvermindering en toekomstvastheid. We werken waar mogelijk samen met regionale partners. Hiermee zorgen we ervoor dat kennis en ervaring worden gebundeld, hergebruik wordt bevorderd en capaciteit zo goed mogelijk wordt verdeeld.

2. Informatie is zoveel mogelijk vrij beschikbaar, bruikbaar en bestendig.
   Uitgangspunt is dat de Provincie open en transparant is. Dat stelt eisen aan de kwaliteit van de onderliggende gegevens. Informatie moet beschikbaar, bruikbaar en bestendig zijn. Zie bijlage 5 voor een nadere toelichting.

3. Eigenaarschap en beheer van processen, data en applicaties is adequaat geregeld.
   Vanuit het oogpunt van kwaliteitsborging ten aanzien van beheer en regie is het beleggen van taken en verantwoordelijkheden voor de verschillende lagen van het informatielandschap van belang. Het moet voor de organisatie duidelijk zijn wie van welke onderdelen de eigenaar is (veelal de manager) en wie er verantwoordelijk is voor het beheer. De taken en verantwoordelijkheden van de eigenaar en beheerder dienen te zijn beschreven. Provincie Zeeland blijft ten allen tijde eigenaar van provinciale gegevens. Samenwerking met leveranciers kan en mag geen verandering brengen in deze verhouding. Dit voorkomt onduidelijkheid over eigenaarschap. Daarnaast wordt leveranciersafhankelijkheid voorkomen en behouden we de regie over provinciale brondata en de archivering hiervan. Voor de verdere uitwerking van het eigenaarschap wordt verwezen naar "Bijlage 3 Eigenaarschap van processen, middelen en informatie".

4. Hergebruik gaat voor standaard gaat voor maatwerk, generiek waar het kan en specifiek waar het moet.
   Voor nieuwe oplossingen wordt eerste gekeken of er al een oplossing beschikbaar is (hergebruik). Is dit niet het geval dan wordt in de markt gezocht naar een standaard oplossing. Alleen als er geen standaard oplossing in de markt is kan maatwerk worden ontwikkeld. Indien er sprake is van een nieuwe oplossing wordt gekeken of deze generiek toepasbaar is.

5. Bij de registratie van provinciale gegevens wordt rekening gehouden met geldende wet- en regelgeving.
   Steeds meer wet- en regelgeving richt zich op de informatievoorziening. Denk daarbij aan de Wet Open Overheid, de Omgevingswet, de Wet Elektronische Publicaties, de nieuwe Archiefwet en de Wet Digitale Overheid, de Wet en regelgeving Basisregistraties, de Algemene Verordening Gegevensbescherming, de Dienstenwet, het Tijdelijk Besluit Digitale Toegankelijkheid overheid. Hiermee wordt bij de inrichting en het gebruik van verschillende componenten rekening gehouden.

6. Servicegerichte architectuur is uitgangspunt.
   Applicaties zijn zo min mogelijk van elkaar afhankelijk. Uitwisseling van gegevens vindt plaats via services op basis van open standaarden. Daarmee ontstaat een flexibel applicatielandschap op basis van het 'loosely coupled' principe, met zo min mogelijk leveranciersafhankelijkheid. Open servicegerichte architectuur is nodig voor samenwerking in de keten. Services en koppelingen zijn functioneel beschreven, servicebeschrijvingen zijn vastgelegd in een service register en/of een service repository. Hiermee houden we overzicht op de functionaliteit van de koppelingen en services.

7. Open standaarden worden toegepast
   Het is van belang dat Provincie Zeeland gevolg geeft aan de implementatie van overheidsbrede adoptiestandaarden vanuit Forum Standaardisatie (Pas toe of Leg uit). Het berichtenverkeer van, naar en binnen Provincies is gebaseerd op de standaarden van het Forum Standaardisatie. Het gebruik van standaarden bevordert toekomstbestendige uitwisseling. Toepassing van dit principe bevordert de interoperabiliteit.

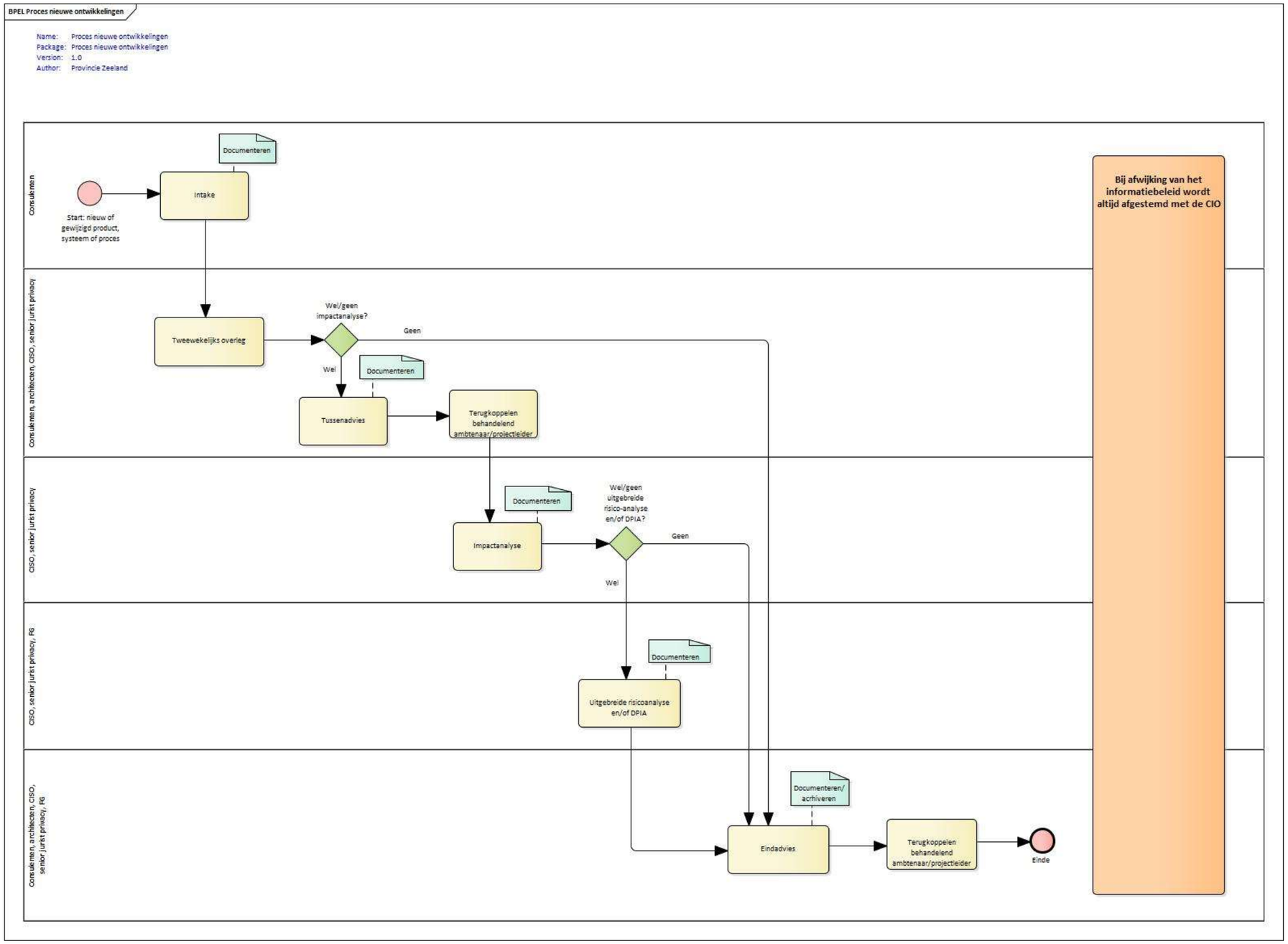
[3] Er is rekening gehouden met de architectuur- en realisatieprincipes van Common Ground van de Vereniging Nederlandse Gemeenten (VNG), zie bijlage 4 voor een nadere toelichting.

8. Open source wordt bij voorkeur en weloverwogen toegepast.
De Provincie Zeeland past bij voorkeur open source toe maar doen dit weloverwogen op basis van functionele behoefte, gebruik bij andere organisaties, beheeraspecten, onderhoud, professionele ondersteuning en kosten/baten. Er wordt aangesloten bij de landelijke agenda van de Digitale Overheid van juli 2018. Een citaat daaruit luidt als volgt: "We willen dat overheidsinformatie en software zoveel mogelijk voor iedereen beschikbaar en toegankelijk is. Open source software verhoogt de transparantie over hoe de systemen van de overheid werken en voorkomt dat we gebonden zijn aan één of enkele leveranciers.".

9. Beheer is adequaat geregeld en werkt volgens standaard methodes.
Functioneel applicatiebeheer, technisch applicatiebeheer en technisch beheer zijn gebaseerd op standaard beheermethodieken (BISL, ASL en ITIL). Dit geldt niet alleen voor het functioneel beheer bij de (centrale) beheerorganisatie, maar ook wanneer functioneel beheer ergens anders in de organisatie is belegd. Wijzigingen worden doorgevoerd conform de vigerende beleidsrichtlijn en bijbehorend sjabloon. Hiermee zorgen we ervoor dat beheer van applicaties en technische infrastructuur op gestructureerde wijze plaatsvindt. Dit komt ten goede aan de betrouwbaarheid en kwalitatieve werking van de informatievoorziening.

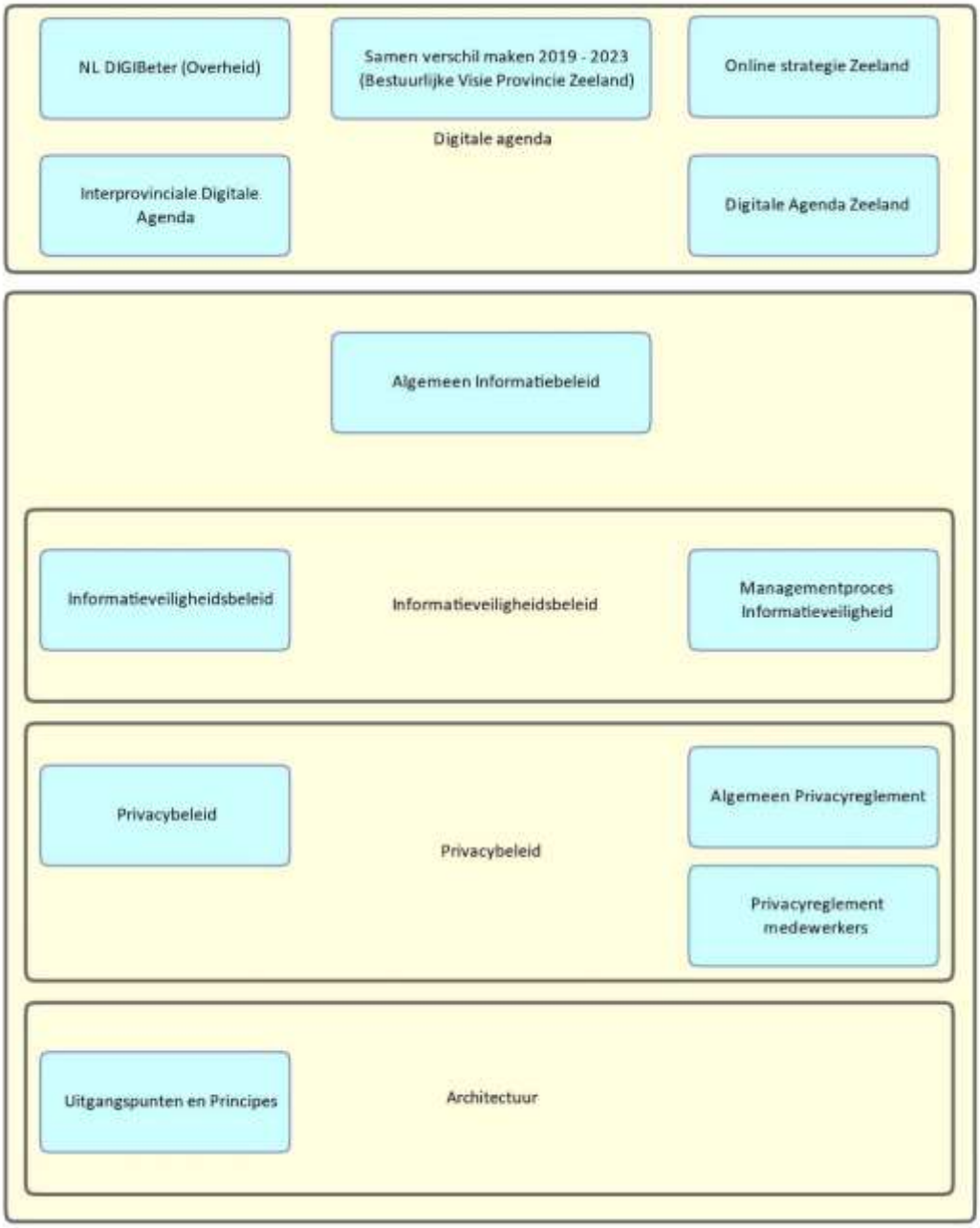
10. Informatieveiligheid en Privacy is geborgd.
Het borgen van informatieveiligheid en privacy is een noodzakelijke voorwaarde bij ontwikkelingen. Het beveiligingsregime dient voor elk soort beleidsinformatie te worden bepaald op basis van risico-afweging. De openheid van informatie dient vergezeld te gaan van een passend niveau van informatiebeveiliging en borgen van privacy. Ontsluiting via services vereist dat dit op een hoog organisatorisch (sturings)niveau wordt verankerd.

BIJLAGE 1: PROCESSCHEMA NIEUWE ONTWIKKELINGEN



Provincie Zeeland

BIJLAGE 2: SAMENHANG INFORMATIEBELEID



BIJLAGE 3: EIGENAARSCHAP

1. Inleiding

Eigenaarschap van processen en van informatie-verwerkende middelen is een van de bouwstenen van een goede informatiehuishouding. Of het nu gaat over informatieveiligheid, datamanagement, wet- en regelgeving of procesontwerp, concreet eigenaarschap zorgt ervoor dat verantwoordelijkheid geborgd wordt en besluitvorming transparant is. In het Informatiebeleid van de Provincie Zeeland zijn als uitgangspunten gesteld:

- eigenaarschap en beheer van processen, data en applicaties is adequaat geregeld.
- de taken en verantwoordelijkheden van de eigenaar en beheerder dienen te zijn beschreven.
- voor elke applicatie (incl. inrichting), dataset en voor elk proces is op managementniveau een eigenaar benoemd die verantwoordelijk is voor de kwaliteit en de actualiteit.

Hiermee zijn drie duidelijke eisen gesteld aan de taken, bevoegdheden en verantwoordelijkheden (TBV's) van een eigenaar: ze zijn *belegd, adequaat geregeld en beschreven*. De eigenaar is een *manager*.
De wijze waarop de adequaatheid wordt vastgesteld en waar de betreffende beschrijving vastgelegd is, is nog niet uitgewerkt. Er is ook nog geen opsomming van de TBV's die relevant zijn voor eigenaarschap.
In het beleid voor informatieveiligheid en het bijbehorende ISMS document ('Managementproces') zijn de TBV's verder uitgewerkt vanuit de invalshoek informatieveiligheid. Het is een generieke beschrijving die van toepassing is op alle eigenaren van processen, gegevens, informatiesystemen en infrastructuren. De opgenomen tekst is al eens eerder getoetst door diverse auditors en zal dus voldoende zijn vanuit het oogpunt van certificering. Echter, idealiter is deze uitwerking een verbijzondering van een (Provincie-)brede definitie die in een bovenliggend informatiebeleid vastgelegd is.
Het doel van deze bijlage is om een aanzet te geven van deze bredere definitie, zodat deze ook in de praktijk verder ingevoerd kan worden dan voor informatiebeveiliging alleen. Per aandachtspunt is een korte paragraaf beschreven. Dit document vormt input voor een verdere afstemming en beoogt niet een 100% antwoord te geven.

2. Uitgangspunten eigenaarschap

In de drie documenten zijn dezelfde uitgangspunten benoemd:

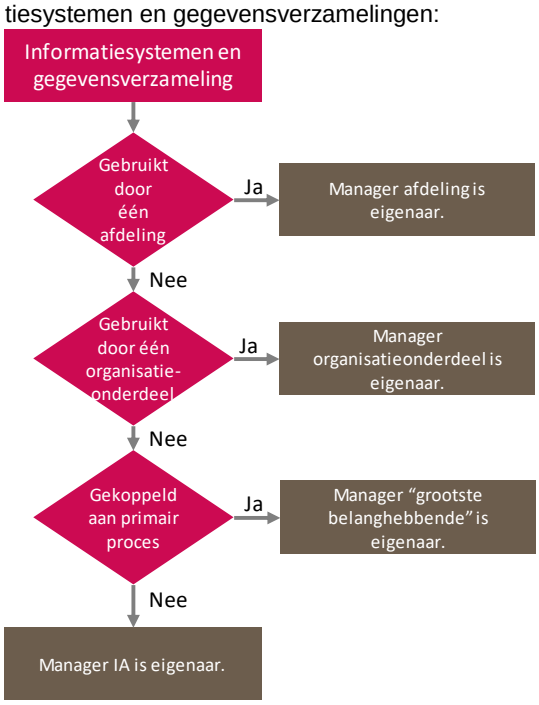
- Voor elk proces, applicatie en dataset is op *managementniveau* een eigenaar benoemd.
- Elke afdelingsmanager, opgavemanager of uitvoeringsprogrammamanager is daarbij zelf verantwoordelijk voor het actueel en betrouwbaar zijn van de door hen gegenereerde en beheerde informatie.

3. Toekenning eigenaarschap

Belangrijke uitgangspunten bij de inrichting van eigenaarschap zijn:

- een eigenaar heeft een belang bij het informatiesysteem, proces, gegevensverzameling etc.;
- eigenaarschap kan niet worden gedeeld;
- de taken van een eigenaar kunnen worden gedelegeerd, niet de verantwoordelijkheid;
- Het proceseigenaarschap wordt gelegd bij de manager die verantwoordelijk is voor de uitvoering van het proces. Vervolgens wordt vastgesteld welke informatiesystemen en gegevensverzamelingen hierbij een rol spelen en wie daarvan de eigenaren zijn.
- de eigenaar van het informatiesysteem of gegevensverzameling heeft het mandaat, het budget en de bijbehorende bevoegdheden om afspraken te maken met proceseigenaren, infrastructuureigenaren en andere belanghebbenden, ten aanzien van functionaliteit, gebruik en beheer.

Provincie Zeeland hanteert de volgende beslisregels voor het toekennen van eigenaarschap van informatiesystemen en gegevensverzamelingen:



- wanneer een informatiesysteem of gegevensverzameling door slechts één afdeling wordt gebruikt, dan is de manager van de afdeling de eigenaar.
- wanneer een informatiesysteem of gegevensverzameling door meerdere afdelingen binnen één organisatieonderdeel wordt gebruikt, dan is de manager van dat onderdeel de eigenaar. De praktische uitvoering van de rol (niet de verantwoordelijkheid) kan belegd worden bij een van de managers van de betrokken afdelingen.
- wanneer een informatiesysteem of gegevensverzameling door verschillende organisatieonderdelen wordt gebruikt, dan is de manager van één van deze organisatieonderdelen de eigenaar op grond van het principe van de 'grootste belanghebbende'. De eigenaar betrekt de overige belanghebbenden intensief bij besluitvorming.
- informatiesystemen, gegevensverzamelingen en infrastructuren die niet aan een primair proces gekoppeld kunnen worden (en die mogelijk als ondersteuning voor de gehele Provincie gelden) hebben (meestal) de afdelingsmanager IA als eigenaar. Denk hierbij aan generieke voorzieningen zoals bijvoorbeeld het datanetwerk, de service bus, de email voorziening, de werkplekken, het documentbeheerssysteem.

4. Scope activiteiten eigenaar

Het eigenaarschap betekent in de praktijk dat de eigenaar de volgende activiteiten inricht of laat inrichten, hierbij ondersteund en geadviseerd door specialisten. Deze door de directie gemandateerde verantwoordelijkheid omvat alle besluiten en activiteiten rond informatieveiligheid gedurende de hele levenscyclus, dus van ontwikkeling/aanschaf tot en met afvoeren. De taken kunnen door de eigenaar voor uitvoering nader gedelegeerd worden naar andere medewerkers. De eigenaar is primair aanspreekpunt voor adviseurs en toezichthouders en legt verantwoording af aan de directie middels de P&C-cyclus.

De taken en verantwoordelijkheden omvatten:

1. bij selectie en aanschaf en ook daarna, periodiek vaststellen van de eisen aan het informatiesysteem of de gegevensverzameling (ook wel BIVP[4] **classificatie** genoemd);
2. uitvoeren van een **risicoanalyse** en/of een **DPIA[5]** op het informatiesysteem of de gegevensverzameling indien nodig;
3. treffen en bewaken van **maatregelen** op het gebied van informatieveiligheid en/of privacy op basis van de risicoanalyse en/of DPIA;
4. laten opnemen van **relevante eisen en afspraken** in contracten, SLA's, verwerkersovereenkomsten, e.d.;
5. controleren dat de eisen en afspraken onder punt 4. daadwerkelijk periodiek gecontroleerd worden op **naleving door de leverancier**;
6. inregelen van de **toegang** tot het informatiesysteem en het beheer hiervan, daar waar vereist door middel van het vaststellen van een autorisatiematrix;
7. besluitvorming over de afhandeling van eventuele **beveiligingsincidenten** betreffende het informatiesysteem;
8. zorgen dat gebruikers de gewenste **opleiding en training** ontvangen;
9. controle op de **juiste werking** van de informatieveiligheids- en privacymaatregelen;
10. mogelijk maken van de uitvoering van de eventuele **rechten van betrokkenen**: bij de verwerking van persoonsgegevens hoort ook dat er verantwoording wordt afgelegd aan de betrokkenen (natuurlijke personen waar het over gaat). De uitoefening van hun rechten –informatie, inzage, rectificatie, beperking van de verwerking, overdraagbaarheid, bezwaar en vergetelheid- verloopt via de eigenaar.
11. toepassen van de **archiveringsregels**, zoals vastgesteld in wettelijke bewaartermijnen en eventueel aanvullend vastgesteld door Provincie Zeeland;

[4] BIVP classificatie betekent: het classificeren van eisen basis van impact op Beschikbaarheid, Integriteit, Vertrouwelijkheid en Privacyaspecten

5 DPIA betekent Data Protection Impact Assessment, dit is een uitgebreide privacy-impactanalyse

12. wanneer (een deel van) het informatiemiddel wordt afgedankt, zorgt de eigenaar dat alle informatie wordt **gemigreerd of vernietigd**.
13. elke eigenaar laat minimaal eens per jaar aantoonbaar een **toets** uitvoeren op actualiteit van zijn eigen informatiehuishouding en of nog wordt voldaan aan actuele eisen t.a.v. architectuur, informatieveiligheid en privacy.

5. Classificatie

- Tijdens het onderzoek naar een nieuw middel voor de informatievoorziening brengt hij/zij eisen die aan het informatiemiddel in beeld en wordt in nauw overleg met afdeling IA en Senior Jurist Privacy een Impactanalyse uitgevoerd (indien nodig gevolgd door een risicoanalyse en/of een DPIA). Die eisen gaan over de beschikbaarheid, integriteit, vertrouwelijkheid, privacy, maximale uitvalduur, maximaal gegevensverlies & de eisen uit de AVG (rechtmatigheid/doelbinding, proportionaliteit, subsidiariteit, dataminimalisatie);
- Aangezien Provincie Zeeland momenteel niet beschikt over een complete classificatie, zullen ook de bestaande middelen alsnog geclassificeerd moeten worden.

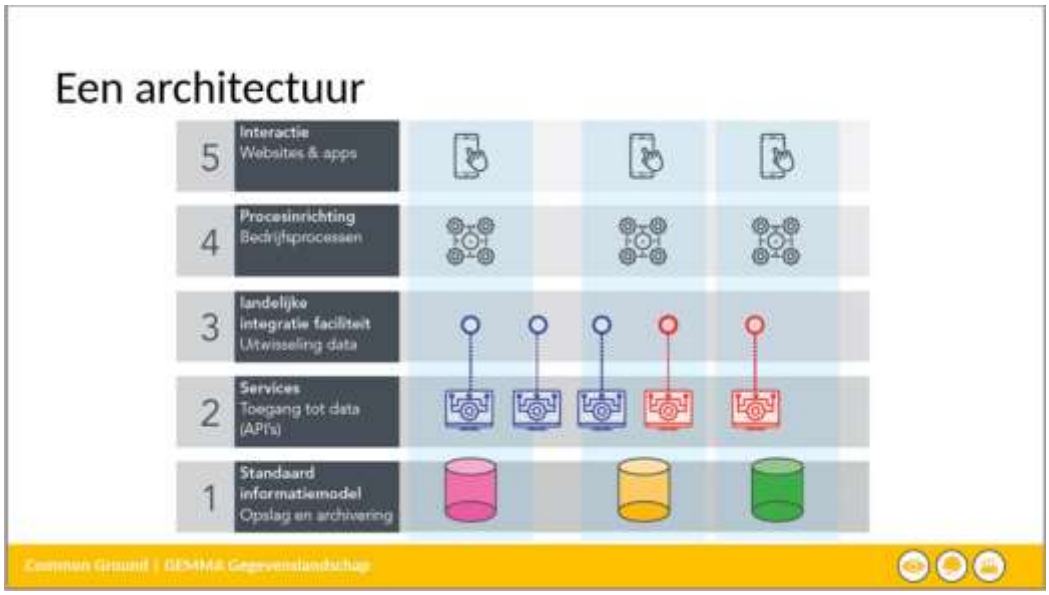
6. Risicomanagement en -maatregelen informatieveiligheid

- De eigenaar is verantwoordelijk voor de uitvoering van een risicoanalyse en/of DPIA voor alle, aan hem toegewezen, kritieke informatiesystemen en gegevensverzamelingen.
- Verder is hij/zij verantwoordelijk voor de vaststelling van de passende beheersmaatregelen en het bepalen van eventuele additionele beheersmaatregelen, bovenop die reeds aanwezig zijn. Hierbij wordt hij/zij ondersteund door de CISO en indien nodig door de Senior Jurist Privacy.
- De beheersmaatregelen worden zodanig geselecteerd dat een optimale balans gevonden wordt tussen veiligheid, kosten en gebruiksvriendelijkheid.
- Het accepteren van alle risico's en restrisico's gebeurt door de eigenaar.
- Alle hoge restrisico's worden ter verificatie en acceptatie voorgelegd aan de CISO en in geval van privacy-risico's de Senior Jurist Privacy en FG. Besluiten door de CISO kunnen eventuele aanpassing van het informatieveiligheidsplan of het treffen van aanvullende beheersmaatregelen inhouden. De eigenaar van het informatiesysteem of gegevensverzameling blijft te allen tijde verantwoordelijk voor alle risico's en de mogelijke consequenties.
- Indien het oordeel van de CISO en voor wat betreft privacy-risico's het oordeel van de Senior Jurist Privacy en FG afwijkt van dat van de eigenaar, dan kunnen de CISO, de Senior Jurist Privacy en FG een aanvullend advies geven aan de CIO. In dat geval neemt de CIO het uiteindelijke besluit in overleg met de CISO en de eigenaar.
- Het komt voor dat maatregelen groter zijn dan het uitvoeren van één of meerdere individuele acties. In dat geval neemt de eigenaar een actie op om een projectvoorstel op te stellen voor de invoering van de betreffende maatregel. Dit projectvoorstel wordt via de hiervoor ingerichte structuren binnen Provincie Zeeland als regulier project ingediend.
- Daar waar afgeweken wordt van een vastgesteld beleid of van standaarden, legt de eigenaar dit vast in een formele verklaring ('comply or explain'). De verklaring bevat een risico-inschatting van de afwijking en de mogelijke consequenties en wordt aan de CISO en indien het de privacy raakt aan de FG gerapporteerd. Hierbij wordt hij/zij ondersteund door specialisten. Afwijkingen zijn alleen toegestaan na uitvoering van een risicoanalyse en met schriftelijke toestemming van de CIO.

7. Registratie van eigenaarschap

Provincie Zeeland beschikt over een actueel en, met de organisatie afgestemd, overzicht van informatiesystemen, eigenaren, leveranciers en beheerders. Dit wordt beheerd door de architecten en vastgelegd in de Enterprise Architectuur tool.

BIJLAGE 4: COMMON GROUND PRINCIPES



BIJLAGE 5: BESCHIKBAAR, BRUIKBAAR EN BESTENDIG

1. Informatie is vrij beschikbaar, tenzij…

Conform het beleid van de Provincie Zeeland is informatie extern openbaar d.w.z. vrij beschikbaar voor iedereen, tenzij:

- er wettelijke belemmeringen zijn in het kader van privacy, vertrouwelijkheid, veiligheid en auteursrechten;
- er persoonlijke beleidsopvattingen van bestuurders, ambtenaren en andere betrokkenen zijn vermeld, die zijn te herleiden naar de persoon;
- er concurrentieverhoudingen kunnen worden geschaad;
- het economisch of financieel belang van de organisatie wordt geschaad.

Voor informatie die niet als extern openbaar geldt, zijn de volgende klassen van toepassing;

- GEHEIM: informatie waarvan de toegang beperkt moet blijven tot een zeer beperkte groep personen, en waarvan compromitteren grote consequenties kan hebben voor de provinciale organisatie en haar werkgebied;
- VERTROUWELIJK: informatie waarvan de toegang beperkt moet blijven tot een beperkte groep personen;
- INTERN OPENBAAR: informatie waarvan het gebruik of de inzage ervan beperkt moet blijven tot de provinciale organisatie.

De Provincie Zeeland werkt intern open en transparant daar waar het kan en sluit aan op het vastgestelde informatieveiligheidsbeleid. Vertrouwelijkheid dient gemotiveerd te worden en zo min mogelijk te worden toegepast (Pas toe of leg uit).

2. Informatie is bruikbaar

Informatie die door de Provincie Zeeland wordt gebruikt, samengesteld en ontsloten moet bruikbaar zijn. Dit houdt in dat de onderliggende gegevens betrouwbaar, correct en (daar waar kan) actueel zijn en op een herleidbare manier worden omgezet naar informatie. Voor het samenstellen, ontsluiten en aanbieden van bruikbare informatie wordt bij voorkeur gebruik gemaakt van open standaarden.

3. Informatie is bestendig

Dit betreft de juridische bestendigheid van informatie, de informatie moet in geval van juridische procedures overeind blijven bij de rechtbank en/of Raad van State. Belangrijk hierbij is dat aandacht word besteed aan de volgende aspecten:

- Datadefinities - welke informatie gebruiken we binnen de organisatie? Wat zijn de beschrijvingen en aan welke technische en functionele eisen moet het voldoen. De datadefinities leg je vast in een bedrijfsgegevensmodel.
- Eigenaar. Wie is de eigenaar van een gegeven? Wie stelt de datadefinities vast? De rol van gegevensbeheerder is hier van belang. Een gegevensbeheerder is een rol die verantwoordelijk is voor het gebruik van de data governance processen om ervoor te zorgen dat de data - zowel de inhoud als de metadata - aan de eisen voldoet.
- Bepaal middels welk proces gegevens worden geregistreerd, geactualiseerd, gecontroleerd en uiteindelijk ook weer worden verwijderd.

Dit fundament is de basis om data goed toe te kunnen passen binnen de organisatie zodat juridische risico’s zo goed mogelijk worden geminimaliseerd.