



WERKORGANISATIE DUIVENVOORDE

www.werkorganisatieduivenvoorde.nl

Informatiebrief

aan de gemeenteraden van Voorschoten en Wassenaar

Zaaknummer : Z/17/005987 en Z/17/005903

Documentnummer :

Datum : 22 februari 2017

Onderwerp : *Beleidsnotitie informatieveiligheid en Informatiebeleidsplan 2017-2020*

Bijlage(n) : *Beleidsnotitie informatieveiligheid en Informatiebeleidsplan 2017-2020*

Geachte Raad,

Steeds meer overheidsdienstverlening vindt tegenwoordig digitaal plaats. Het belang van goede informatiebeveiliging wordt daarmee steeds groter. Daarom is er vanuit de VNG een normenkader opgesteld voor gemeentebrede informatiebeveiliging: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Het gemeentelijke veiligheidsbeleid wat hieruit voortkomt, moet lokaal worden vastgesteld en geïmplementeerd.

Goede resultaten

De Werkorganisatie Duivenvoorde vindt informatiebeveiliging belangrijk. Sinds 1995 wordt de Basisregistratie Personen op veiligheid ge-audit. Ook de paspoort- en rijbewijzenverstrekking, de Basisregistratie Adressen en Gebouwen en de drie DigiD-aansluitingen van de werkorganisatie en de beide gemeenten, zijn tot nu toe altijd succesvol ge-audit.

Daarnaast is er ook hard gewerkt aan veilige e-mail, een veilig wifi-netwerk, een veilige thuiswerkoplossing, verbeterde procedures in-/uit-dienst en screening personeel, het beheer van mobiele apparatuur en het jaarlijks uitvoeren van uitwijktesten voor interne omgeving en cloud-omgeving. Taken en rollen in de informatiebeveiliging zijn vastgesteld en functionarissen benoemd/aangewezen. Informatieveiligheid is expliciet opgenomen in de portefeuille van één van de leden van het Dagelijks Bestuur van de WODV en verantwoording hierover wordt sinds 2014 afgelegd in een apart onderdeel van de paragraaf bedrijfsvoering in de jaarrekening van de WODV.

Als bestuur zijn wij dan ook trots op de geleverde prestaties en gemaakte stappen.

Informatieveiligheidsbeleid

In het rapport Digitale Dienstverlening constateert de Rekenkamercommissie dat er resultaten geboekt worden maar dat het lokale beleidsmatig kader ontbreekt. Daarom hebben de gemeenteraden van Voorschoten en Wassenaar toegezegd om direct aan de slag te gaan met de aanbevelingen uit het onderzoek. In 2016 zijn we dan ook gestart met het vormgeven van een beleidscyclus voor gemeentebrede informatieveiligheid. Er is een beleidsnotitie informatieveiligheid opgesteld die voldoet aan de eisen die de BIG stelt aan een informatieveiligheidsbeleid. De punten die in de notitie naar voren komen, vormen de basis voor de verdere ontwikkeling van informatiebeveiliging. De beleidsnotitie informatieveiligheid is als bijlage toegevoegd.

Informatieveiligheidsanalyse en Informatiebeveiligingsplan 2017

Er is een informatieveiligheidsanalyse gemaakt. Die vergelijkt de huidige situatie met de norm die is vastgelegd in de BIG. De veiligheidsanalyse geeft aan dat de Werkorganisatie Duivenvoorde zich qua invoering van de BIG op het landelijk gemiddelde bevindt.

De door het dagelijks bestuur van de Werkorganisatie Duivenvoorde vastgestelde informatieveiligheidsanalyse is niet bijgevoegd. Omdat het document een beeld geeft van de lokale situatie rondom informatieveiligheid, is het strikt vertrouwelijk.

De volgende stap is om het beleid te concretiseren en inzichtelijk te maken welke nog in te voeren maatregelen (directe) actie nodig hebben. Hieruit komt een Informatiebeveiligingsplan 2017 waarin wij prioriteiten voorstellen met daarbij een kostenraming. Dit plan wordt in een later stadium voorgelegd aan het dagelijks bestuur van de Werkorganisatie Duivenvoorde en wordt jaarlijks aan de actualiteit aangepast.

Informatiebeleidsplan 2017-2020

Het Informatiebeleidsplan 2017-2020 beschrijft het informatiebeleid van de gemeenten Voorschoten en Wassenaar en de Werkorganisatie Duivenvoorde voor de periode 2017-2020. Het informatiebeleid is nauw verweven met de visie op dienstverlening, de bedrijfsvoering en uiteindelijk de rol die de gemeenten willen spelen voor inwoners en ondernemers. Het dagelijks bestuur van de Werkorganisatie Duivenvoorde is verantwoordelijk voor het vaststellen en uitvoeren van het Informatiebeleid.

Het Informatiebeleidsplan bepaalt voor de komende vier jaar de koers die de informatisering en automatisering van de gemeenten en de Werkorganisatie Duivenvoorde volgt. Deze koers is intern (collegeplannen, concernplan, teamplannen ect.) en extern (landelijk programma Digitaal 2017 en de Digitale agenda 2020) uitgezet. Het beleidsplan wordt jaarlijks aan de actualiteit aangepast. In de jaarrekening van de Werkorganisatie Duivenvoorde wordt verantwoording afgelegd over de voortgang van de uitvoering van het informatiebeleid.

Het ontbreken van het beleidsmatig kader voor het informatiebeleid is eveneens als constatering opgenomen in het rapport Digitale Dienstverlening van de Rekenkamercommissie. Met het vaststellen van het informatiebeleidsplan 2017-2020 door het dagelijks bestuur van de Werkorganisatie Duivenvoorde wordt voldaan aan de aanbeveling van de Rekenkamercommissie. Het Informatiebeleidsplan is als bijlage bijgevoegd.

Met vriendelijke groet,

Het Dagelijks Bestuur van de Werkorganisatie Duivenvoorde,



de conerndirectie,
M.H. van der Veer



de voorzitter,
Ch. B. Aptroot

Informatie Beleidsplan 2017-2020



**Gemeente
Voorschoten**

Gemeente  **Wassenaar**



WERKORGANISATIE DUIVENVOORDE

Inhoud

Management samenvatting	1
Visie: de gemeente flexibel, innovatief en wendbaar in 2020	2
Trends en Ontwikkelingen	3
Gemeenten, politiek en de VNG	3
Nora, Gemma, Digitaal 2017, Digitale Agenda 2020 en GDI	3
GDI	3
Archetypen: de richting van de gemeenten en de WODV scherp bepalen	4
De belangrijkste vraagstukken t.a.v. dienstverlening, bedrijfsvoering en informatisering en ICT	5
Extern gerichte, innovatieve dienstverlening	7
Doorontwikkeling innovatief dienstverleningsconcept	7
Dienstverlening door bundeling van krachten in het sociaal domein	9
Omgevingswet: één loket voor de burger voor de openbare ruimte	11
Geografische kaarten als visitekaartje van de gemeente	13
Digitale transformatie: het nieuwe werkterrein van de gemeente	15
Digitale transformatie	15
Toepassing digitale transformatie: de participatiemaatschappij	16
Webcare: #gemeente	17
Big data ten behoeve van beleidsvalidatie en beleidsbepaling	18
Smart City	19
Hoe kan ik altijd en overal mijn werk doen?	20
Digitaal samenwerken, papierarm, intern en extern	20
Het Nieuwe Werken / Sociale innovatie	21
Applicatierationalisatie: werken onder architectuur	21
ICT-outsourcing	23
Outsourcing van de automatisering	23
Automatisering en IT-beheer	23
Applicatielandschap en koppelingen (informatisering)	23
I&A-medewerkers	23
De basis op orde	24
Gebruik van basis- en kerngegevens	24
Informatie voldoende beveiligd	25
Lean-IT: procesoptimalisatie binnen ICT	26
Gezond boerenverstand en ICT	27
De I&A-architectuur visualiseert de ontwikkelopgave	27
GEMMA 2	28
Hoe: de veranderopgave voor I&A-medewerkers en organisatie	29

Management samenvatting

Dit document beschrijft het Informatiebeleid van de gemeenten Voorschoten en Wassenaar en de Werkorganisatie Duivenvoorde voor de periode 2017-2020. Het informatiebeleid is nauw verweven met de visie op dienstverlening en de bedrijfsvoering, en uiteindelijk de rol die de gemeenten willen spelen voor inwoners en ondernemers. De Werkorganisatie Duivenvoorde (WODV) is verantwoordelijk voor het uitvoeren van het Informatiebeleid. In dit document wordt daarom afwisselend gesproken over de gemeenten (strategisch) en de WODV (tactisch en operationeel)

Gemeentelijke visie

Voorschoten en Wassenaar (de gemeenten) willen een gedegen en continu niveau van dienstverlening bieden zonder grote financiële pieken en dalen, ook al worden er steeds nieuwe grote wetgevingen uitgerold over gemeenten. Dit willen ze bereiken met een flexibele en wendbare bedrijfsvoering en dienstverlening uitgevoerd door de Werkorganisatie Duivenvoorde. Voor de WODV en haar medewerkers betekent dit dat verandering een continue factor is. Daarom wordt de organisatie ingericht om optimaal de regie te voeren ([archetype flexibel en wendbaar](#)).

De Dienstverlening van de gemeenten wordt op hoofdlijnen als volgt ingericht:

- Dienstverlening is gericht op snelheid en duidelijkheid met slimme e-formulieren (Leveringszekerheid)
- Regels zijn er om iets voor inwoners te betekenen i.p.v. ze te beperken in hun mogelijkheden (Waardecreatie)
- Minimalisering van bureaucratie; deregulering, processen zijn lean (Complexiteitsreductie)
- Inwoners en medewerkers moeten zichzelf in de meeste situaties zelf kunnen redden (Zelfservice)
- Een globaal klantbeeld bevindt zich op MijnOverheid.nl en een gedetailleerd beeld in de backoffice (Klantbeeld)
- Veel (eenvoudige) producten gaan digitaal. Face-to-face contact is mogelijk voor complexe producten (Differentiatie)

(Referentie: Implementatieplan dienstverlening 2015-2017)

De Bedrijfsvoering van de WODV wordt op hoofdlijnen als volgt ingericht:

- Flexibiliteit en modulariteit in de bedrijfsvoering is gericht op vakdomeinen (Meerschalligheid)
- Medewerkers worden verder ontwikkeld: taakvolwassen, creatief en proactief, digitaal vaardig (Empowerment)
- De WODV streeft in alles naar een vaste kern en een flexibele schil (Schaalbaar)
- De bedrijfsvoering is digitaal tenzij en is digitaal duurzaam (Digitaal)
- Diensten en de mogelijkheid tot werken worden plaats- en tijd onafhankelijk aangeboden (Sociale Innovatie)

(Referentie: Concernplan en Jaarplan WODV)

Een optimale dienstverlening wordt bereikt door inwoners te (ver)leiden naar MijnOverheid.nl. Als de burger gedetailleerde informatie wil, verstrekt de backoffice deze.

De gemeenten profileren zich als een actieve (participatieve) overheid. De afdelingen PU en POI/I&A van de WODV ondersteunen initiatieven van inwoners op het terrein van digitale middelen, kennis en kunde. De WODV ontwikkelt kennis en kunde op de nieuwe, innovatieve IT-vakgebieden zoals digitale transformatie, big data, Internet of Things, webcare en Smart City technieken. Deze kennis kan worden aangewend om vakafdelingen te ondersteunen bij o.a. het realiseren van de participatiemaatschappij, beleidsvorming en beleidsvalidatie.

De WODV zet verder stevig in op standaardisatie van informatiestromen om het werken in ketens efficiënter en effectiever te maken. Ook de landelijke ontwikkelingen binnen het programma Digitaal 2017 en de Digitale agenda 2020 worden omarmd en als belangrijk fundament gezien voor de informatievoorziening van de gemeenten.

Omdat steeds meer applicaties uit de cloud komen zal de komende jaren worden onderzocht of de technische automatisering van de WODV kan worden uitbesteed (outsource). De behoefte aan een eigen server-infrastructuur neemt af. De informatisering van de gemeenten en beleidskwesties worden in **samenwerking** met andere partijen (gemeenten, KING, VNG) opgepakt en doorontwikkeld om de toenemende complexiteit het hoofd te bieden.

Om bovengenoemde transformatie te kunnen volgen worden andere eisen gesteld aan de I&A medewerkers, van beheer naar toepassing en advies. Met de toevoeging van het applicatiebeheer aan de functie van systeembeheer is daar al een aanvang mee gemaakt.

Visie: de gemeente flexibel, innovatief en wendbaar in 2020

Zijn de inwoners en ondernemers van Voorschoten en Wassenaar tevreden over de gemeentelijke dienstverlening? Wordt er al inhoud gegeven aan de “participatiemaatschappij”? Is er een verandering in het dienstverleningsconcept onder invloed van decentralisaties en de naderende Omgevingswet? Wordt er geanticipeerd op de ontwikkeling van de cloud? Hoe succesvol is de invoering van zaakgericht werken in de organisatie? En is Het Nieuwe Doen al meer geworden dan flexwerken, heeft het daadwerkelijk een cultuurverandering tot stand gebracht? Is de organisatie nu slagvaardiger naar de toekomst toe?

In al deze ontwikkelingen en processen speelt informatievoorziening en ICT een belangrijke rol. Het gebruik van mobiele devices, clouddiensten, apps, sociale media, big data, smart city toepassingen en de beschikbaarheid van breedband-internet verandert in een hoog tempo de manier waarop inwoners en overheid met elkaar communiceren en gegevens uitwisselen. Al deze ontwikkelingen roepen de vraag op hoe lokale overheden kunnen omgaan met snelle en continue veranderingen. En dat in een netwerksamenleving waarbij flexibele organisatievormen, die kunnen uitbreiden en krimpen, de nieuwe norm lijken te zijn.

De ‘continue verandering’ vraagt om een nieuwe kijk op de inrichting van de organisatie, waarbij aandachtsgebieden meer in samenhang opgepakt worden. Meerschalligheid, adaptief vermogen, innovatie en taakvolwassen medewerkers zijn hierbij sleutelbegrippen om de organisatie van de toekomst in te richten. Een krachtige informatievoorziening is daarin een strategisch middel.

Dit IBP geeft richting aan het informatiebeleid voor de komende 4 jaar, rekening houdend met:

- De wens om als gemeenten en WODV innovatief, flexibel en wendbaar te opereren (VNG, Gemeenten op weg naar 2020, 2015)
- Initiatieven voor digitalisering vanuit het Rijk zoals [Digitaal 2017](#), [Dienstverlening 2020](#) en de [Digitale Agenda 2020](#) (Ministerie van Economische Zaken, 2013), (Bas Eenhoorn, 2015) (Ronald Plasterk, 2013)
- Nieuwe wetgeving (VNG, Dossiers decentralisaties sociaal domein, 2015), (Omgevingswet, 2014)
- Technische trends en ontwikkelingen (Europese unie, 2014), (Microsoft, 2015).

Ondanks de focus op informatievoorziening, kan en mag dit document niet los gezien worden van de vraagstukken op het gebied van bedrijfsvoering, procesoptimalisering en dienstverlening (zie het negen-vlaks model). Deze discussie dient dan ook integraal gevoerd te worden met het management (WODV) en portefeuillehouders (dagelijks bestuur en gemeenten).

Dit document formuleert I&A-beleid voor de gemeenten en de WODV op een voor management, bestuur en colleges leesbare manier om zo de verbinding te leggen tussen I&A en de organisatie.

ICT is daarmee niet alleen een verplicht nummer, maar een belangrijk middel om organisatiedoelen te bereiken.

	Bedrijfsvoering Dienstverlening	Informatie Management	ICT diensten Automatisering
Strategisch (richten)	Visie op bedrijfsvoering dienstverlening	Visie op I i-strategie	Visie op A a-strategie
Tactisch (inrichten)	Management en organisatie Procesontwerp	Informatie- en applicatie architectuur	Technische architectuur
Operationeel (verrichten)	Functioneel beheer	Gegevens beheer	Technisch beheer

Trends en Ontwikkelingen

Gemeenten, politiek en de VNG

In alle regio's van het land heeft de VNG gesprekken gevoerd met wethouders, griffiers, raadsleden en secretarissen. Daar zijn steeds drie vragen gesteld:

1. Wat moet er veranderen om de aansluiting tussen samenleving en lokaal bestuur te vinden en te behouden?
2. Wat kunnen gemeenten zelf en welke randvoorwaarden hebben ze daarbij nodig?
3. Wat zijn lokale of regionale vraagstukken en wat willen we als gemeenten de komende jaren samen oppakken?

Versterken en vitaliseren (VNG)

Uit de bijeenkomsten kwam een duidelijke rode draad: we willen de lokale democratie versterken en vitaliseren. Dat leidt tot een krachtige lokale overheid. Dit is dan ook de ambitie voor de VNG en daarmee bepalend voor de strategie en de collectieve agenda. Dat leidde weer tot een aantal hoofdthema's waar gemeenten samen aan werken, waaronder:

- De veranderende samenleving vraagt om nieuwe verhoudingen, om een overgang van een hiërarchische naar een vloeibare horizontale samenleving.
- De ontwikkelingen in de samenleving vragen om een nieuwe rol van gemeenten: de gemeente als spil tussen partijen en de gemeente die vraag gestuurd werkt.
- Nieuwe vraagstukken vragen om een ander beeld van bestuurlijk Nederland met samenwerkingsvormen op meerdere schaalniveaus. Maar het borgen van de lokale democratie blijft altijd het uitgangspunt.
- En tot slot: de randvoorwaarden. Het lokaal bestuur krijgt te maken met complexe vraagstukken en heeft daarbij financiële ruimte nodig.

Nora, Gemma, Digitaal 2017, Digitale Agenda 2020 en GDI

Informatiebeleid van gemeenten is voor een belangrijk gedeelte gebaseerd op de GEMMA-architectuurprincipes. De principes van deze architectuur zijn de afgelopen jaren veelvuldig besproken en geïmplementeerd, ondanks het feit dat de realisatie niet altijd evident c.q. praktisch mogelijk is.

Dit document gaat deze principes niet herhalen, maar verwijst graag naar http://www.gemmaonline.nl/in-dex.php/Overzicht_GEMMA_Architectuurprincipes.

Daarnaast zijn er diverse visiedocumenten vanuit de rijksoverheid gepubliceerd waarmee ook de gemeentelijke I&A agenda wordt bepaald. Deze zijn hier terug te vinden: [Digitaal 2017](#) en de [Digitale Agenda 2020](#)

GDI

Definitie van de GDI

De generieke digitale infrastructuur van de overheid (GDI) bestaat uit standaarden, producten en voorzieningen die gezamenlijk gebruikt worden door (alle) meerdere overheden, vele publieke organisaties en in een aantal gevallen ook door private partijen.

- De GDI is een onmisbaar deel van de (digitale) basisvoorzieningen waarmee organisaties hun primaire processen inrichten.
- De GDI is, naar zijn aard, niet organisatie-, sector- of domeinspecifiek.

De GDI bestaat uit herbruikbare digitale basisvoorzieningen, standaarden en producten die het overheden, publieke organisaties en private partijen mogelijk maken om hun primaire processen doelmatig in te richten en te blijven ontwikkelen. De GDI is een dynamisch geheel welke de komende jaren gewijzigd kan worden door de ontwikkeling van nieuwe generieke voorzieningen en standaarden of door het uit productie nemen van al opgenomen voorzieningen.

Archetypen: de richting van de gemeenten en de WODV scherp bepalen

Voordat het informatiebeleid opgesteld kan worden, is het van belang om een scherpe richting te kiezen voor de toekomst van de gemeenten en de WODV. In de praktijk is het doorgaans lastig om een richting te bepalen als de consequenties niet goed inzichtelijk zijn. In dat geval is het moeilijk kiezen voor bestuurders, directie en management. Op het moment van schrijven van deze nota speelt er een aantal zaken die het moeilijker maken een goed toekomstbeeld te formuleren. Zo zijn er; de voorgenomen nauwere samenwerking van Voorschoten met de Leidse regio, de aan de WODV opgelegde bezuinigingen en de centrale huisvesting van het ambtelijk apparaat.

Het gebruik van Archetypen is een goed middel gebleken om keuzes te maken en de consequenties te overzien. Het model van de archetypen is ontwikkeld in samenspraak met diverse gemeenten, die wilden weten hoe de missie en visie vertaald kunnen worden naar diverse dienstverlening- en bedrijfskundige aandachtsgebieden zoals management, cultuur, ict, finance, hrm en organisatie. De onderkende archetypen voor gemeenten zijn:

1. Maximaal dienstverlenend
2. Innovatief en modern
3. Kostenbewust en sober
4. Flexibel en schaalbaar
5. Traditioneel

Geen enkele gemeente heeft een complete match met één van de archetypen. Maar er is altijd wel meer herkenning en affiniteit met één van de vijf. Ook dient men zich te realiseren dat gemeenten feitelijk niet meer op zich zelf staan maar altijd onderdeel zijn van meerdere samenwerkingsverbanden en onderdeel zijn van een keten. In die gevallen zijn archetypes meer van toepassing op vakdomeinen of ketens.

Door nu het scenario door te lopen van een visie op dienstverlening (wat voor gemeente willen we zijn voor onze inwoners en ondernemers), via de daaruit af te leiden visie op bedrijfsvoering (hoe gaan we die dienstverlening leveren, wat betekent het voor mensen en middelen) kan de vertaling gemaakt worden naar het informatiebeleid (wat voor systemen hebben we dan nodig, hoe richten we het in, welke eisen worden gesteld) en de automatisering (welke infrastructuur is er nodig, welke apparaten zullen ingezet worden).

Uitgaande van de ter beschikking staande beleidsstukken (collegeprogramma's, visie op de dienstverlening, concern- en jaarplan WODV) is voor dit informatiebeleidsplan de primaire archetype "Flexibel en schaalbaar" en secundaire archetype "Innovatief en modern" van toepassing. Daarmee wordt uiteraard nog steeds een zeer goede dienstverlening geleverd en wordt er op de financiën gelet. Maar de pure focus (die je kunt uitleggen aan medewerkers en inwoners) is gericht op flexibiliteit en schaalbaarheid, zodat er langjarig continuïteit in dienstverlening en financiële stabiliteit ontstaat. Deze wens komt voort om de snelle veranderingen in de maatschappij het hoofd te kunnen bieden: verandering lijkt een continue factor. De archetype kan nu vertaald worden naar een aantal basisprincipes:

1. Dienstverlening is gericht op snelheid en duidelijkheid (Leveringszekerheid)
2. Regels zijn er om iets voor inwoners te betekenen i.p.v. ze te beperken in hun mogelijkheden (Waardecreatie)
3. Er is kennis over regievoering en het voorkomen van bestuurlijke drukte (Governance)
4. Flexibiliteit en modulariteit in de bedrijfsvoering is gericht op vakdomeinen (Meerschalligheid)
5. Minimalisering van interne bureaucratie, deregulering, processen zijn lean (Complexiteitsreductie)
6. Inwoners en medewerkers moeten zichzelf in de meeste situaties zelf kunnen redden (Zelfservice)
7. Veel producten moeten digitaal, face-to-face contact is mogelijk voor complexe producten (Differentiatie)
8. De organisatie mag fouten maken en er wordt gestuurd op langjarig resultaat (Leiderschap)
9. Medewerkers worden verder ontwikkeld: taakvolwassen, creatief en proactief en digitaal vaardig (Empowerment)
10. Interne en externe ontwikkelingen worden actief gemonitord en jaarlijks geëvalueerd (Alert)
11. De WODV streeft in alles naar een vaste kern en een flexibele schil (Schaalbaar)
12. De gemeenten bouwen aan realistische financiële buffers voor tijden dat het nodig is (Buffer).
13. De bedrijfsvoering is digitaal tenzij en is digitaal duurzaam ingericht (Digitaal)
14. Diensten en de mogelijkheid tot werken wordt plaats- en tijd onafhankelijk aangeboden (Sociale Innovatie)

In de volgende hoofdstukken worden bovengenoemde basisprincipes toegepast op de bedrijfsvoering, dienstverlening en ICT/informatievoorziening in 2020.

De belangrijkste vraagstukken t.a.v. dienstverlening, bedrijfsvoering en informatisering en ICT

Na de relatieve duidelijkheid van het concept Antwoord in de voorbije jaren, lijkt het tijd om diverse beleidsvelden van gemeenten grondig te herijken. De volgende onderwerpen hebben de komende 5 jaar een stevig effect op de dienstverlening, bedrijfsvoering en informatievoorziening:

1. Wat zijn de verplichtingen die opgelegd worden vanuit de Rijksoverheid vanuit het programma Digitaal 2017? Denk aan de wet Generieke Digitale Infrastructuur (wGDI), de wet Elektronisch Bestuurlijke Verkeer (Awb), de aanpassing aan de Bekendmakingswet en de wetgeving eID-stelsel en publiek eID middelen. Vooral de wGDI (als opvolger van NUP) bevat de nodige verplichtingen zoals een aansluiting op mijnoverheid.nl voor alle gemeenten.
2. De gevolgen van decentralisaties in het sociale domein (3D's) en de openbare ruimte(omgevingswet) op de gemeentelijke organisatie zijn fors. Denk aan het effect op de organisatie, dienstverlening, informatiebehoefte, verantwoording en aansturing. Dus hoe gaat de gemeente om met: één gezin, één plan, één regisseur binnen het sociale domein en één ontwikkelplan, één omgevingsloket, één vergunning binnen de openbare ruimte?
3. Het werken in ketens wordt een steeds grotere uitdaging. De gemeente is niet noodzakelijkerwijs de eerste of meest nabije overheid, maar veel meer een schakel in een keten. In bijvoorbeeld het sociale domein vindt signalering van sociale problematiek (of de vraag van een burger) plaats op tal van plaatsen zoals bij het CJG, bij het UWV, de huisarts, de politie, op school, bij orgaanbieders, en zorgverleners, etc. De gemeente is onderdeel van een uitgebreid netwerk. Klantroutes variëren, afhankelijk van het startpunt. Uitwisseling van informatie zal nog meer gestandaardiseerd moeten plaatsvinden. Dit vereist dat de gemeente een doelarchitectuur (SOLL) ontwerpt die toekomstige interactie met ketenpartners faciliteert.
4. Het concept Antwoord heeft zijn langste tijd gehad: de relatie tussen de gewenste dienstverlening en de gewenste bedrijfsvoering als vertrekpunt voor de inrichting van het Klant Contact Centrum, de implementatie van zaakgericht werken en het bouwen aan een klantbeeld zorgt voor een nieuwe uitdaging. Het is tijd voor Antwoord 2.0.
5. De rol van de gemeente in de Digitale Transformatie: er zijn steeds meer maatschappelijke kwesties die (deels) opgelost worden door digitale mogelijkheden te benutten. Denk aan het gebruik van drones, het gebruik van sensoren binnen de zorg, big-data toepassingen t.b.v. beleidsondersteuning en validatie, het gebruik van smart-city toepassingen om de leefbaarheid te vergroten. Maar ook het volgen en wellicht modereren van discussies op social media over gemeentelijke gebeurtenissen (bijvoorbeeld rondom vluchtelingenprobleem). Welke rol pakken de gemeenten?
6. Het feit dat steeds meer vakapplicaties als Software as a Service (SAAS) worden aangeboden en de beschikbaarheid van nieuwe standaarden zorgen voor een totaal nieuw gedistribueerd applicatielandschap. Dit heeft een flink effect op de benodigde ICT-infrastructuur, de rollen en functies van de I&A-medewerkers en de bedrijfszekerheid van de totale bedrijfsvoering. De WODV zal over de cloud-ontwikkeling zeker een standpunt in moeten nemen.
7. Digitale weerbaarheid, privacy en informatieveiligheid, digitale volwassenheid en digitale duurzaamheid zijn allen aan elkaar gerelateerde onderwerpen waarbij de gemeente en haar medewerkers bewust en zorgvuldig om moet gaan met haar gegevens. Deze onderwerpen bevatten allen een prominente zachte factor waarbij medewerkers informatiebewust en digitaal volwassen gemaakt moeten worden. Naast de richtlijnen en wetgeving (Baseline Informatiebeveiliging Gemeenten, wet bescherming persoonsgegevens, wet datalekken, archiefwet) is er dus behoefte om medewerkers bij te scholen op het terrein van techniek en ICT. Anders wordt de kloof tussen de organisatie en de mogelijkheden c.q. gevaren die ICT levert onoverbrugbaar.
8. Zoeken en vinden van informatie wordt een steeds grotere uitdaging. Informatie is overal aanwezig (o.a. dms, persoonlijke schijf, dropbox), in verschillende vormen (office, pdf, email, xml), op verschillende informatiedragers (usb, smartphones, tablets) en in verschillende versies, beheerd door verschillende mensen of groepen mensen. Het beheer van al deze informatie en het vermogen om de juiste relevante en betrouwbare gegevens terug te

vinden (enterprise search, collaboration tools) wordt een steeds grotere uitdaging en kost een substantieel deel van de productieve tijd.

9. In zijn algemeenheid is er een streven naar verlaging van de kwetsbaarheid, een verhoging van de kwaliteit en grip houden op de kosten. Hiervoor zijn diverse strategieën om dat te bereiken: samenwerking met andere gemeenten en harmonisatie van applicaties, applicatierationalisatie, outsourcing van taken, procesvereenvoudiging, etc. Het algemene streven naar complexiteitsreductie begint bij de business.
10. Het gebruik van social media neemt nog steeds toe. Inmiddels zitten er 1.7 miljard mensen op Facebook. Social media wordt niet alleen ingezet om te communiceren, maar ook om meldingen (openbare ruimte) door te geven. Inwoners gebruiken het onderling om de veiligheid in de buurt te verbeteren (Whatsapp). Anderzijds zijn er ook grote groepen mensen die zich via social media organiseren. Voor overheden is het van belang om deze ontwikkelingen te volgen. Ook de Wet Electronisch Bestuurlijk Verkeer speelt hier een rol. Diverse gemeenten hebben daarom al de functie Webcare in het leven geroepen. De vraag is ook of en hoe interne gemeentelijke systemen gekoppeld kunnen of moeten worden.
11. Het gebruik van mobile devices neemt hand over hand toe. Ook de ontwikkeling en gebruikersvriendelijkheid van Apps neemt een grote vlucht (appifisering). Vroeger maakte je in de trein een praatje, nu kijkt iedereen op zijn smartphone. Gemeenten worden geconfronteerd met ondernemers die nieuwe diensten ontwikkelen (buitenbeter, WOZ-bezwaar) en gemeenten moeten hier een antwoord op formuleren. En de kans dat de smartphone de werkplek van de toekomst wordt is zeer groot.
12. Misschien wel de belangrijkste: de komende jaren gaat de rol van de I&A-organisatie binnen gemeenten drastisch veranderen: door samenwerking, door outsourcing, door nieuwe taken (o.a. digitale transformatie), de behoefte aan meer managementinformatie. Soms zijn niet alle I&A-medewerkers meer nodig omdat taken veranderen of verdwijnen. Er ontstaat een behoefte aan andere (en nieuwe) kennis, nieuwe competenties en ervaringen. Dit vereist een langetermijnvisie.

Extern gerichte, innovatieve dienstverlening

Om diensten te leveren, vinden er activiteiten plaats op vijf aandachtsgebieden: organisatie, proces, informatie, applicatie en gegevens. Het beleid is erop gericht om inwoners een innovatieve en moderne klantervaring te geven, doordat producten en diensten op een persoonlijke, betrouwbare en slimme manier worden geleverd.

Doorontwikkeling innovatief dienstverleningsconcept

(Kernwoorden: zelfservice, leveringszekerheid, moderne dienstverleningskanalen)

Er is een tendens om de dienstverlening te baseren op een klant die zelfstandig in staat is om een situatie te beoordelen (zelfstudie) en indien nodig zelfstandig of samen acties uit te zetten (zelfservice). Die trend is onder andere bij banken al jaren zichtbaar. Het kan het best worden geïllustreerd aan de hand van 'het Hypotheekdossier' van de Rabobank. In eerste instantie verzamel je als klant alle relevante informatie in 'het Hypotheekdossier'. Op basis van deze informatie en eventueel rekenhulp weet je welke hypotheekvormen het best aansluiten bij jouw behoefte. Dit heet zelfstudie. Op het moment dat je daadwerkelijk een hypotheek wilt afsluiten kun je een afspraak maken. Je bespaart kosten als je de benodigde documenten zelf toevoegt aan het dossier, zelfservice. Een andere vorm van zelfservice is het online afsluiten van de hypotheek.

Met name repeterende en eenvoudige dienstverleningsprocessen lenen zich voor geautomatiseerde afhandeling, zonder menselijke tussenkomst.

Inwoners willen hun productaanvragen regelen, op een voor hen prettig tijdstip, waarbij volledige duidelijkheid wordt gegeven over wat er mogelijk is. Dit vereist slimmere formulieren of apps, gekoppeld met backofficesystemen, die al direct gerichte antwoorden kunnen geven. De al in gebruik zijnde huwelijksapp is een mooi voorbeeld: kies de datum, de trouwlocatie, de ambtenaar, en de zaalinrichting, en de burger krijgt direct antwoord of dit mogelijk is en de huwelijksdatum kan online worden vastgelegd.

Voor complexe producten (o.a. vergunningen) wordt een face-to-face contact als prettig ervaren.

Om medewerkers en samenleving optimaal te faciliteren, is het goed om de informatiestromen te bundelen rondom een persoon of een situatie. Zo kan men zelfstandig een situatie beoordelen (zelfstudie) en indien nodig zelfstandig (zelfservice) of samen (collaboratie) acties uitzetten.

Om dienstverlening te faciliteren, is het van belang om de status van een productaanvraag te kennen. Alle productaanvragen en alle contactmomenten vormen een klantbeeld. Dit beeld kan eventueel opgebouwd worden uit deelklantbeelden vanuit de verschillende vakdomeinen.

De volgende uitgangspunten worden gehanteerd:

- Alle zaken van alle afdelingen in het zaak-data-magazijn met een globale status.
- Innovatie vindt plaats via big-data binnen het zaak-data-magazijn (data-driven).
- Koppeling zaak-data-magazijn met MijnOverheid.nl.
- De detail status van aanvragen bevindt zich in het vakdomein.
- Contactenregistratie vindt plaats in de backoffice.
- Alle documenten worden verzameld in de midoffice.
- Het e-loket/e-formulieren worden ook door het KCC gebruikt.

Doelstelling

- Doelstelling voor de gemeenten en de WODV: proactieve, innovatieve dienstverlening die gericht is op leveringszekerheid.
- Doelstelling voor de I&A-afdeling: een innovatieve doelmatige informatie- en applicatiearchitectuur in dienst van het dienstverleningsconcept.

Richtlijnen

- De WODV streeft naar een domeinspecifiek klantbeeld en een globaal centraal klantbeeld
- Vragen worden binnen de organisatie doorgestuurd, niet de klant.
- Binnen en tussen samenwerkingsverbanden worden servicenormen voor dienstverlening vastgelegd.
- MijnOverheid.nl is de primaire bron voor het klantbeeld.
- Alle dienstverleningskanalen geven de burger direct een vaste opleverdatum en informatie over leveringsmogelijkheden zodat de vragen over de voortgang van aanvragen meetbaar afnemen.
- Digitale kanalen (zoals website, apps, social media) zijn de voorkeurs dienstverleningskanalen voor snel-klaar en eenvoudige producten.
- Kanalen waar face-to-face contact mogelijk is (zoals balie, chat-mogelijkheden en video conferencing) zijn de voorkeurskanalen voor complexe producten.
- De organisatie wil met behulp van het globaal klantbeeld inzicht hebben in alle binnengekomen aanvragen en de doorlooptijden van alle aanvragen.
- Aanvragen worden toegewezen aan een afdeling/team, niet aan een persoon, om leveringszekerheid te vergroten.
- Klanten kunnen kiezen uit diverse contactvormen zoals spraak, tekst of beeld.
- Klanttevredenheid wordt gemeten.
- De organisatie leert van gestelde vragen van inwoners, ondernemers en instellingen.
- De gemeenten maken maximaal gebruik van landelijke portalen en voorzieningen.
- Bij een samenwerking wordt de overdracht van informatie een integraal onderdeel van de samenwerkingsovereenkomst om de dienstverlening te optimaliseren.
- De websites bestaan grotendeels uit een selfservicedesk.



Consequenties

- De WODV herijkt de werking van de frontoffice en het zaakgericht werken (zie volgende sectie).
- Aanvraagformulieren, apps, en andere digitale kanalen worden zo intelligent mogelijk gemaakt om ervoor te zorgen dat de klant direct uitsluitsel krijgt over leveringsmogelijkheden en opleverdata.
- De gemeenten voeren Unified messaging¹ in t.b.v. klantcontacten.
- De gemeenten stellen servicenormen op met gegarandeerde leveringstijden.
- De gemeenten stellen richtlijnen op voor het toelaten van nieuwe digitale kanalen (apps, social media, etc.).
- Alle afspraken (dus niet alle contacten) met inwoners, ondernemers en instellingen worden vastgelegd.
- Er is een speciaal meetsysteem voor klanttevredenheid.
- Face-to-face gesprekken kunnen opgenomen (beeld en/of geluid) en gearchiveerd worden.
- De gemeente implementeert tools om de diverse kanalen te monitoren en aan te sturen (zie webcare).
- Dienstverlening aan huis wordt ondersteund door een volledige toegang tot de werkomgeving.

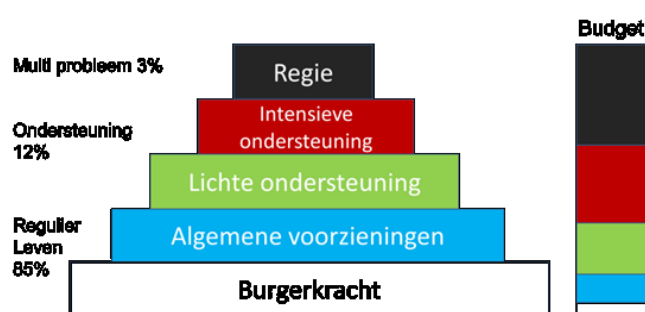
¹ Onder unified messaging (UM) verstaat men het mechanisme waarbij inkomende berichten, zoals spraak, tekst, fax, e-mail, video, in een gemeenschappelijke inbox worden opgeslagen en geregistreerd. De berichten in die inbox kunnen vervolgens met een willekeurig apparaat worden geraadpleegd, gewijzigd en beantwoord.

Dienstverlening door bundeling van krachten in het sociaal domein

De filosofie achter de decentralisaties in het sociale domein bestaat uit drie onderdelen die zijn samengevat in één slogan: één gezin, één plan, één regisseur:

1. Doordat gemeenten integraal verantwoordelijk zijn voor zorg, welzijn en onderwijs, zal men meer in staat zijn om overzicht te krijgen op de situatie van een gezin of een cliënt. Door het betere overzicht kan een escalatie van problemen voorkomen worden (vroeg signalering c.q. preventie bij gestapelde problematiek)
2. Men introduceert het principe van Eigen Kracht; dit betekent dat er niet gekeken wordt wat cliënten en gezinnen niet meer kunnen en waarbij eerder nog aanvullende zorg geregeld werd (compensatiebeginsel), maar veel meer naar wat cliënten en gezinnen nog wel kunnen (zelfredzaamheid).
3. Tegelijkertijd wordt de oplossing voor cliënten en gezinnen meer gezocht in algemene voorzieningen dan in maatwerk. Elke gemeente dient te beschikken over een lokale basis-zorg-infrastructuur, die bestaat uit maatschappelijke partijen, (sport)verenigingen, buurtverenigingen, etc. om er voor te zorgen dat cliënten minder snel doorstromen naar de duurdere professionele zorg: de participatiemaatschappij.

De verdeling van taken om “één gezin, één plan en één regisseur” mogelijk te maken, kunnen eenvoudig verdeeld worden op basis van de zorgpyramide: de onderste twee lagen (burgerkracht en algemene voorzieningen) zullen lokaal georganiseerd moeten worden (de lokale basis zorg infrastructuur) en de professionele zorg (de bovenste drie lagen) worden regionaal georganiseerd.



De informatievoorziening van de decentralisaties wordt daarmee bepaald door 4 belangrijke vraagstukken:

- Dossievorming: Hoe krijgen we het dossier rondom één gezin compleet? Hoe leveren ketenpartners, maatschappelijke partners en de gemeente alle gegevens aan? Hoe gaat de regisseur werken met deze gegevens?
- Operatie en IT-integratie: Hoe wordt de dienstverlening en informatievoorziening geïntegreerd in respectievelijk de frontoffice en de gemeentelijke IT-architectuur? Wordt het zakenmagazijn gebruikt voor het vastleggen van het dossier? Of wordt een nieuw systeem geïntroduceerd voor case-management (regiesysteem)?
- Sturing en verantwoording: Hoe worden financiële cijfers en zorg-cijfers gebundeld om te kunnen sturen? Of t.b.v. de uitkering uit het gemeentefonds? Hoe krijgen we gegevens van onze ketenpartners?
- Analyse en vroeg signalering: Als het dossier compleet is, met welke analysetechnieken wordt preventie en vroeg signalering geïmplementeerd? Welke gegevens zijn daar voor nodig? (Big data)

Om de informatievoorziening vorm te geven zijn er in principe drie strategieën mogelijk:

1. Laat zorgaanbieders en ketenpartners zorgdragen voor de informatiesystemen
2. Centraliseer alle informatie bij de gemeente om één volledig dossier te krijgen
3. Een combinatie van de twee bovenstaande

Doelstelling

- Doelstelling voor de gemeenten: één gezin, één plan, één regisseur, verhogen zelfredzaamheid en participatie van inwoners en lagere zorgkosten, uitbesteding van 3D-taken
- Doelstelling voor de WODV/I&A: faciliteren van slim ingerichte processen, ondersteunen van experimenten en gemakkelijke en veilige uitwisseling van gegevens over organisatiegrenzen heen.

Richtlijnen

- Inwoners kunnen zelf online werken/input leveren aan hun zorgplan
- Inwoners hebben zicht op de door de gemeente over hen vastgelegde gegevens
- Medewerkers in sociaal (wijk)teams kunnen gemakkelijk samenwerken aan een casus
- Het aanbod van basisvoorzieningen is actueel, volledig en gemakkelijk te raadplegen
- Medewerkers, inwoners en ketenpartners weten welke betaalde zorg via de gemeente kan worden verstrekt
- Bij het inzetten van betaalde zorg is er inzicht in kosten en kwaliteit per aanbieder

- Lopende en reeds doorlopen aanvragen en zorgtrajecten zijn bekend
- Medewerkers krijgen ruimte om ervaring op te doen met nieuwe werkwijzen en van elkaar te leren.

Consequenties

- Invoering van een regiesysteem, dat gebruikt wordt door sociale wijkteams en het SoZa-KCC en ketenpartners.
- Online beschikbaar maken van het regiesysteem voor cliënten, zorgaanbieders en ketenpartners.
- Koppelen van systemen van zorgaanbieders/ketenpartners aan de ICT-architectuur van de gemeenten.
- Implementatie van de zelfredzaamheidsmatrix.
- Het Regiesysteem is gekoppeld met het financiële systeem en de systemen voor werk en inkomen, WMO en Jeugdzorg t.b.v. uitwisseling van product- financiële- en zorg-gerelateerde gegevens.

Omgevingswet: één loket voor de burger voor de openbare ruimte

De Omgevingswet, die naar verwachting in 2019 in werking treedt, integreert 26 wetten op het gebied van de fysieke leefomgeving en heeft als uitgangspunt: minder en overzichtelijke regels, meer ruimte voor initiatieven, lokaal maatwerk en vertrouwen.

Inwoners, ondernemers en overheden zijn betrokken bij de uitvoering van de Omgevingswet. Door de toenemende integra- liteit neemt de noodzaak van gegevensuitwisseling tussen de actoren toe. Tot 2024 wordt gewerkt aan het Digitaal Stelsel Omgevingswet (DSO). Het DSO ondersteunt de informatie-uitwisseling met ketenpartners, maar ook de proces- sen voor planvorming, vergunningverlening, toezicht en handhaving bij de overheid. Bestaande voorzieningen, werk- wijzen en standaarden worden waar mogelijk gebruikt. Het stelsel van verbonden databronnen, die processen met informatie gaan voeden, speelt ook hier ook een belangrijke rol.

HET NIEUWE OMGEVINGSSTELSEL

De 4 verbeteringen

Een vernieuwend stelsel van instrumenten die met elkaar samenhangen, gebundeld in een Omgevingswet. Voor een inzichtelijk, voorspelbaar en gemakkelijk te gebruiken omgevingsrecht. Die samenhang in beleid, besluitvorming en regelgeving mogelijk maakt. Ondersteund door een actieve en flexibele overheid en een snellere en betere besluitvorming.



Door online inzicht te bieden, kunnen inwoners, ondernemers, maatschappelijke organisaties en overheden alle beschik- bare informatie ophalen. Met één klik op de kaart is de juiste informatie over een bepaald gebied beschikbaar voor de gebruiker (Factsheet Digitaal stelsel Omgevingswet, 2015).

De gemeente zal moeten investeren in nieuwe IT-voorzieningen: onder andere een webportaal (voor toegang tot het DSO), een landelijke registratie van omgevingsdocumenten (voor inzicht in geldende regels), het Informatiehuis Ruimte en een gegevenscatalogus (een overzicht van diensten die via het stelsel worden geboden). Bestaande voor- zieningen moeten verder aangepast worden: Omgevingsloket Online, Activiteitenbesluit Internet Module (AIM) en Ruimtelijke plannen.

Visie VNG/KING

Vanaf 2019 hebben gemeenten een aantal voorzieningen nodig om met de Omgevingswet te kunnen werken. Het gaat onder meer om een webportaal (voor toegang tot het DSO), een landelijke registratie van omgevingsdocumenten (voor inzicht in geldende regels), het Informatiehuis Ruimte en een gegevenscatalogus (een overzicht van diensten die via het stelsel worden geboden). Daarnaast worden de bestaande voorzieningen Omgevingsloket Online (OLO), Activiteitenbesluit Internet Module (AIM) en Ruimtelijke plannen geschikt gemaakt voor de Omgevingswet.

Collectief gemeentelijke digitaliseringsprojecten (UIVO-CG)

De UIVO CG-projecten werken de consequenties van en eisen aan Informatievoorziening & ICT uit die voortkomen uit de Omgevingswet en het DSO vanuit gemeentelijk perspectief; in relatie tot andere relevante inrichtingsaspecten, in

de ruime omgeving van het gemeentelijke werkveld en voor zover er draagvlak is voor een collectieve aanpak.

Aan de gemeentelijke kant:

- Worden de informatiekundige consequenties van de wet- en regelgeving, de instrumenten van de Omgevingswet en het Regelbeheer uitgewerkt.
- Worden de (veranderingen in de) gemeentelijke processen vastgelegd, ook in relatie tot regionale samenwerkingen (OD's, Veiligheidsregio's, GGD's, etc.). Dit sluit aan op het interbestuurlijke invoeringsproject Uitvoeringsvarianten, waarin onderzocht wordt of hierin een aantal standaardvarianten kan worden afgesproken.
- Worden de gevolgen voor de (inrichting van de) gemeentelijke [dienstverlening](#) bepaald en er worden een aantal serviceformules geformuleerd.
- Wordt de informatiearchitectuur gemodelleerd in relatie tot het DSO en de informatiehuizen.
- Wordt de applicatiearchitectuur gemodelleerd en de eventuele benodigde standaarden en koppelvlakken gedefinieerd.

Om bovenstaande resultaten te verkrijgen, worden projecten uitgevoerd. Daarnaast zijn er nog projecten die randvoorwaardelijk zijn: Relatiemanagement, Leveranciersmanagement en Privacy & Informatiebeveiliging. Uitwerking Informatievoorziening Omgevingswet Interbestuurlijk (UIVO-I)

Onder UIVO-I vallen alle digitaliseringsprojecten waarvoor het noodzakelijk is dat meerdere overheidslagen met elkaar tot resultaten komen waar ze hun commitment aan kunnen geven. Dit gaat verder dan 'afstemmen en tussentijds uitwisselen', zoals in de VIVO-fase.

Op interbestuurlijk niveau:

Wordt inzicht verkregen in de keten: samenwerking, processen, zaaktypen, producten- en dienstencatalogus, etc. Dit bepaalt de contactpunten met de processen en zaken van de bevoegde gezagen en stelt derhalve eisen aan de informatievoorziening vanuit DSO en de inrichting van de informatievoorziening van de bevoegde gezagen.

Worden eisen in kaart gebracht aan het DSO en omgekeerd: vanuit de functionele en technische inrichting van het DSO bepalen welke eisen aan de informatievoorziening en ICT van de bevoegde gezagen worden gesteld.

Doelstelling

- Doelstelling voor de gemeenten: Het tijdig voorbereiden en aanpassen van de organisatieonderdelen om in 2019 te voldoen aan de Omgevingswet.
- Doelstelling voor de WODV/I&A: Het mogelijk maken dat er kan worden aangesloten op het digitale loket, informatieregisters en de infrastructuur die nodig is om informatie uit te wisselen.

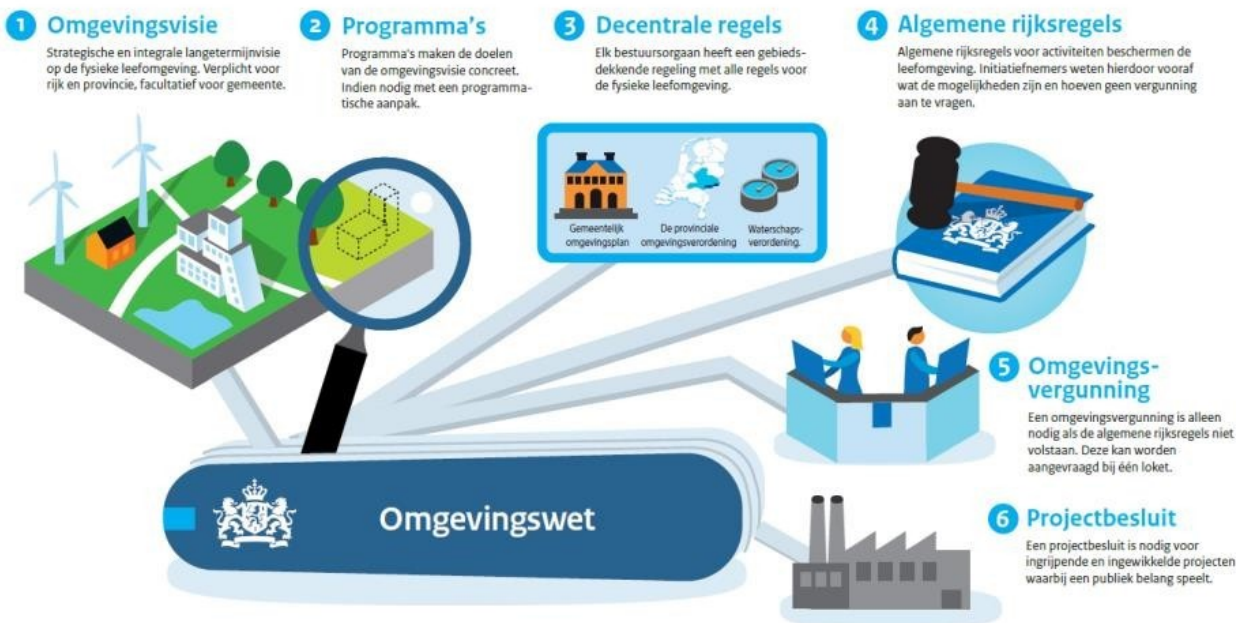
Richtlijnen

- Zoveel mogelijk processen worden ingericht volgens landelijke richtlijnen en standaarden.
- De gemeenten zijn tijdig en goed geïnformeerd.
- De afdeling Ruimtelijke Ordening neemt de lead.

Consequenties

- Aanvullende richtlijnen voor de omgevingswet worden opgesteld naar aanleiding van VIVO (Verkenning Informatie Voorziening Omgevingswet).
- Gegevens over de openbare ruimte die van belang zijn voor het correct uitoefenen van het bevoegd gezag worden geïnventariseerd.
- Er moet worden geïnvesteerd in nieuwe voorzieningen t.b.v. Omgevingswet.
- Bestaande voorzieningen moeten geschikt worden gemaakt voor de Omgevingswet.

De 6 instrumenten



Geografische kaarten als visitekaartje van de gemeente

Geografische informatie neemt een steeds grotere plaats in in de informatievoorziening van gemeenten, zeker ook met de introductie van de Omgevingswet. Geografische kaarten, gemaakt via geografische informatie-systemen (GIS) zijn een visueel aantrekkelijk middel om prestaties van verschillende bestuurslagen of gemeentelijke organisaties te vergelijken. Door gemeentelijke prestaties te visualiseren kunnen nieuwe conclusies worden getrokken. Als prestaties tegen elkaar afgezet worden en gerelateerd worden aan de omvang van een probleem, kan een uitspraak gedaan worden of het gevoerde beleid werkt. Voorbeelden:

- Met GIS kan het beleid m.b.t. de decentralisaties per wijk/dorp vergeleken worden
- Met GIS kan inzicht worden verkregen in het aantal BOR-meldingen per wijk/dorp
- Met GIS kan eenvoudig inzicht gegeven worden in relevante informatie voor de burger/bedrijf vanuit zijn woonlocatie gezien: vergunningen, wegwerkzaamheden, bestemmingsplannen (www.ruimtelijkeplannen.nl), zorginstellingen (www.socialekaartnederland.nl), WOZ-waarden, demografische gegevens, etc.

Doelstelling

- Doelstelling voor de gemeenten: inzetten van geografische informatie voor dienstverlening en de visualisatie van beleidseffecten en beleidsbepaling.
- Doelstelling voor de WODV/ I&A: inrichten, opleveren en aanbieden van geografische gegevens t.b.v. ruimtelijke analyses (GIS) en dienstverlening.

Richtlijnen

- De gemeenten koppelen zoveel mogelijk een locatiecode aan administratieve gegevens uit o.a. het sociale domein, zorg, openbare ruimte (MOR) en algemene dienstverlening.
- Geografische informatie en -systemen worden gebruikt om de verbinding te leggen tussen diverse informatiebronnen ten behoeve van het helpen oplossen van ruimtelijke vraagstukken.
- De gemeenten hanteren zoveel mogelijk geografische standaarden.
- De gemeenten gaan actief aan de slag met ruimtelijke analyses (GIS).

Consequenties

- Inventarisatie van reeds beschikbare geografische informatie die vervolgens vindbaar en toegankelijk wordt gemaakt;
- Informatie met een geo-component wordt beter gedeeld, waardoor er beter kan worden samengewerkt met het hoogheemraadschap/waterschap, de provincie en de nutsondernemers.
- De beschikbare informatie wordt toegankelijk gemaakt voor derden, waardoor samengewerkt kan worden met ketenpartners en/of derden die diensten verlenen (aannemers, ingenieursbureaus e.d.), ook met het oog op de omgevingswet.
- Informatie wordt op de websites aangeboden aan inwoners over 'wat speelt in de buurt', met name in relatie tot het kern- en buurtgericht werken: werkzaamheden, omleidingen, herinrichtingsplannen.
- Een Geo-portaal wordt ingericht t.b.v. aannemers en inwoners met o.a. huisaansluitingen, BOR meldingen, Meldpunt openbare Ruimte. De meldingen over de openbare ruimte worden thematisch weergegeven per kern, buurt en straat.
- GIS wordt ingezet met betrekking tot het efficiënt en effectief uit kunnen voeren van de diverse beheertaken.



Digitale transformatie: het nieuwe werkterrein van de gemeente

We leven in een ondernemende, sociaal bewogen en techniek gedreven maatschappij. Binnen de samenleving van de gemeenten starten er dagelijks initiatieven die bijdragen aan een betere samenleving. Ondersteuning van de gemeenten kan daarbij welkom zijn. Hoe nodig je jezelf als gemeente uit bij deze initiatieven en hoe maak je optimaal gebruik van de (denk)kracht van de samenleving en de digitale wereld? Deze ontwikkelingen, samengevat in de term “*digitale transformatie*”, raken een fundamentele vraag voor alle I&A-afdelingen van gemeenten: in welke mate moet de I&A-afdeling betrokken zijn? Welke expertise is er nodig om deze nieuwe vakgebieden te omarmen? De behoefte vanuit beleidsmakers om iets te doen met de digitale transformatie is er zeker.

De volgende secties geven uitleg waar de digitale transformatie over gaat en het beleid dat een gemeente er voor kan ontwikkelen.

Digitale transformatie

Digitale transformatie gaat over het effect van ICT op alle aspecten van de maatschappij en de organisatie. Van apparaten die werk uit handen nemen tot het opnieuw inrichten van werkprocessen omdat apparaten onderdelen hebben overgenomen. ICT maakt zaken mogelijk i.p.v. dat ICT alleen maar volgend is. En vaak zijn de uitkomsten verrassend en onvoorspelbaar. Daarom spreekt men over de “digitale transformatie”.

In de digitale transformatie streeft men naar een organisatie die met digitale middelen en digitaal volwassen medewerkers haar bedrijfsdoelstellingen behaalt. Denk bijvoorbeeld aan ondernemers zoals Spotify, Uber en AirBnB. Digitaal en bedrijfsdoelstellingen zijn hier zodanig aan elkaar gekoppeld dat de digitale invulling van het primaire proces het businessmodel heeft beïnvloed. Deze vorm van transformatie is voor gemeenten in het algemeen (nog) niet in zicht. Wel kan de gemeente delen van taken of processen met behulp van ICT transformeren. Ter inspiratie vijf voorbeelden van samenwerking met de samenleving die ondersteund worden met behulp van digitale middelen:

1. Crowdlabor, het uitbesteden van een taak aan de samenleving. De archieftaak om metadata toe te voegen aan bijvoorbeeld foto's wordt op de site www.velehanden.nl uitgevoerd. Geïnteresseerden over de hele wereld kunnen hieraan bijdragen.
2. Crowdfunding, het financieren van een project door de samenleving. Voetbrug, de Luchtsingel in Rotterdam werd door veel kleine bijdragen, in diverse vormen, gefinancierd.
3. Crowdvoting, besluitvorming door de samenleving. Gemeente Dordrecht liet meer dan 4000 inwoners meedelen over een bezuinigingsvoorstel van € 3 miljoen.
4. Crowdcollaboration, meewerken aan een taak. Gemeente Nijmegen formuleerde met meer dan 1000 inwoners het cultuurbeleid.
5. Crowd competition, een oplossing creëren in competitievorm. Provincie Utrecht organiseerde samen met onder andere Utrechtinc, een hackathon. Een competitie waarin een energie app werd ontwikkeld.



De luchtsingel in Rotterdam

Door ICT wordt een groter bereik gecreëerd waardoor het uitbesteden van onderdelen van taken of processen een reële optie wordt. Door gestructureerd en structureel taken en of processen op deze manier samen op te pakken met de samenleving maakt een gemeente optimaal gebruik van inwoners, ondernemers en medewerkers. Zo transformeert ze naar de (digitale) gemeente van de toekomst.

Doelstelling

- Doelstelling voor de gemeenten: het gemeentelijke businessmodel transformeren door structureel en gestructureerd taken met behulp van digitale mogelijkheden samen met de samenleving uit te voeren.
- Doelstelling voor de WODV/I&A: de vakafdelingen ondersteunen bij het uitvoeren van projecten die gericht zijn op digitale transformatie.

Richtlijnen

- De gemeenten voeren tenminste een digitaal transformatieproject uit per jaar om te ervaren en te leren.
- De WODV/I&A coördineert actief de ICT van het (extern gerichte) project.
- De gemeenten (I&A-afdeling en vakafdelingen) weet waar ze het over heeft als het gaat om de digitale transformatie en het actief betrekken van inwoners.
- Projecten die in het kader van digitale transformatie worden uitgevoerd, worden zorgvuldig gemeten en geëvalueerd. Leasons learned worden actief meegenomen bij het volgende project.

Consequenties

- Er wordt budget vrijgemaakt voor digitale transformaties
- De gemeente experimenteert met interactieve beleidsvorming in de opiniërende fase van besluitvorming
- Er wordt gemeten in hoeverre het gebruik van nieuwe digitale middelen bijdraagt aan het realiseren van strategische doelen.

Toepassing digitale transformatie: de participatiemaatschappij

De gemeente streeft naar een sterke 'participatiesamenleving' of Civil Society. Een Civil Society is een samenleving waarin mondig inwoners vooral zelf (zonder tussenkomst van politieke partijen of overheden) voor hun belangen en idealen opkomen, al dan niet door zich te organiseren. Een voorbeeld zijn dorpsraden met een bescheiden budget en ambtelijke ondersteuning. De ICT-ondersteuning van de participatiemaatschappij bestaat uit diverse onderdelen:

- Het versterken van de technische infrastructuur ten dienste van de participatiemaatschappij
- Het verbeteren en vermeerderen van de diensten op dit netwerk.
- Het bieden van advies en ondersteuning aan projecten vanuit de samenleving
- Een budget vrijmaken specifiek gericht op de toepassing van ICT t.b.v. de participatiemaatschappij

Hierop is bovendien de wet van Matcalfe van toepassing. *'De waarde van een netwerk (lees civil society) neemt kwadratisch toe met het aantal aangesloten apparaten.'* Denk bijvoorbeeld aan het gebruik van smartphones en het aantal gebruikte smartwatches.

Investeren in een Civil Society, benaderd vanuit het ICT-perspectief, kan dan bijvoorbeeld door:

- Te investeren in de technische infrastructuur: Next Generation Access (o.a. glasvezel) projecten of snelle 5G verbindingen
- Te investeren in (nieuwe) services die op dit netwerk worden aangeboden.

Hiermee ontstaat een fundament op basis waarvan inwoners en ondernemers nieuwe activiteiten ontplooiën en zichzelf organiseren.

De "Andere Handen Community" van de o.a. de gemeente Bodegraven-Reeuwijk is een mooi voorbeeld waarbij men in de zorg van de toekomst gebruik wil maken van slimme technologie. O.a. social media wordt benut, zodat zelfregie en samenredzaamheid bevorderd wordt.

Het woord Domotica is een samentrekking van domus (woning) en telematica en staat voor elektronische communicatie tussen allerlei elektrische toepassingen in de woning en woonomgeving ten behoeve van bewoners en dienstverleners. Dit wordt steeds vaker toegepast ter ondersteuning van het langer zelfstandig blijven wonen van ouderen en gehandicapten.

Een ander mooi voorbeeld is de beveiliging van buurten en ondernemersterreinen. Meer innovatieve projecten zijn te vinden op depilotstarter.vng.nl

Doelstelling

- Doelstelling voor de gemeenten: verduurzamen van de participatie samenleving met behulp van digitale middelen.
- Doelstelling voor de WODV/I&A: Het faciliteren van initiatieven m.b.t. de participatiemaatschappij.



Richtlijnen

- De WODV/I&A neemt kennis van en adviseert over initiatieven op het terrein van de participatiesamenleving. (o.a. gegevensbeveiliging)
- De gemeenten stellen zich positief op tegenover initiatieven en experimenten met betrekking tot de participatiemaatschappij.
- De gemeenten initiëren tenminste één project per jaar gericht op burgerparticipatie met een ICT-component.

Consequenties

- Medewerkers nemen kennis van de (digitale) mogelijkheden van de participatiemaatschappij
- De WODV/I&A ontwikkelt kennis en adviesvaardigheden t.a.v. het gebruik van (digitale) samenwerking en e-participatie
- Er wordt een samenwerkingstool (Viadesk, SharePoint, Smartsheet, All-fresco, etc.) ingevoerd voor gemeente én inwoners

Webcare: #gemeente

WhatsApp, LinkedIn, Facebook en YouTube zijn niet meer weg te denken uit ons digitale leven en dit is slechts een greep uit het nieuwe medialandschap. Door deze nieuwe media te monitoren weet iedereen wat er leeft in de samenleving. Ook geeft het meer inzicht in de personen en daarmee de kennis, vaardigheden en netwerk van personen. Zowel in de samenleving (via Facebook) als de gemeentelijke organisatie (LinkedIn).

Veel overheden experimenteren volop met nieuwe media. Gemeenten zijn toegankelijk via WhatsApp, Facebook, Twitter, LinkedIn en YouTube. Het brengt de overheid dichterbij de (jonge) burger. Toepassingen variëren van het informeren van inwoners tot aan het gebruik als dienstverleningskanaal o.a. voor het doen van meldingen.

Dit vraagt een actief beleid van de gemeente op deze media. De twee belangrijkste beleidskwesties zijn:

1. Omdat nieuwe media een nieuw dienstverleningskanaal vormt, zal er aandacht geschonken moeten worden aan vraagstukken zoals het koppelen en vastleggen van contactmomenten met inwoners en nieuwe informatiestromen aan bestaande ICT-systemen. Immers, een melding via Twitter zal uiteindelijk wel netjes afgewerkt en terug gerapporteerd moeten worden.
2. Omdat ideeën en sentimenten van de samenleving verwoord worden via sociale media, zal hierop actief naar geluisterd en gereageerd moeten worden. Een veelgebruikte term voor het managen van interactie met de samenleving via diverse (digitale) media is community management.

Doelstelling

- Doelstelling voor de gemeenten: proactieve houding t.a.v. nieuwe media om te signaleren, informeren, beïnvloeden, beleid te bepalen en als dienstverleningskanaal.
- Doelstelling voor de WODV/I&A: koppelen van bestaande informatiesystemen aan nieuwe media en ervoor zorgen dat nieuwe media informatie voldoet aan vigerende wetgeving (Archiefwet, WEBV, WBP).

Richtlijnen

- De gemeenten managen de interactie met de samenleving via diverse (digitale) kanalen en media (kanaalsturing).
- De gemeenten openen specifieke kanalen wel, en bepaalde kanalen niet voor dienstverlening (beleidskeuze).
- Medewerkers hebben de mogelijkheid om te werken in samenwerkingstoepassingen zoals LinkedIn, Facebook, Twitter, op mobiele apparaten, ook al worden deze niet door de gemeente ondersteund.
- De WODV ondersteunt medewerkers met behulp van eenvoudige richtlijnen hoe om te gaan met nieuwe media vooral in relatie tot de participatiesamenleving.

Consequenties

- Bepalen op welke wijze nieuwe media worden toegelaten binnen het informatiedomein van de gemeenten.
- Servicenormen ten aanzien van nieuwe media (denk aan reactietijden) worden bepaald.
- Er wordt beleid ontwikkeld ten aanzien van community management i.s.m. communicatie en het MT.
- Nieuwe dienstverleningskanalen worden gekoppeld aan de ICT-architectuur van de gemeente.
- De WODV meet in hoeverre het gebruik van nieuwe media het gebruik van andere kanalen beïnvloedt.
- De WODV meet in hoeverre het gebruik van nieuwe media de klantervaring en –waardering beïnvloedt.

Big data ten behoeve van beleidsvalidatie en beleidsbepaling

Mensen, apparaten en slimme sensoren generen een ongelooflijke hoeveelheid data. Data over het gebruik van producten, openbare ruimte, individuen, groepen mensen, uit machines, vervoers- en energiestromen. Door de huidige computerkracht is het mogelijk om van de bulk van data, real time informatie te genereren.

Big Data zijn datasets die niet met reguliere database management systemen onderhouden kunnen worden. De datasets worden gekenmerkt door: Volume (schaal van data), Velocity (snelheid van analyse van actuele (streaming) data) en Variety (verschillende type data). Overige kenmerken zijn: Veracity (betrouwbaarheid van (het gebruik) van datasets) en diens Value (waarde van data)

Zo is het mogelijk om via sociale media te monitoren wat het sentiment van de dag is over een bepaald onderwerp (o.a. [google trends](#)). Big Data kan ook een signaal afgeven. Zouden kinderen die in armoede opgroeien vaker ziek zijn en met de WMO in aanraking komen? Het geeft gebiedsgericht werken een nieuwe dimensie. Vrijwel iedereen is voorzien van een mobiel apparaat met GPS-functionaliteit.



Het analyseren van deze big data, patronen daarbinnen herkennen, vertalen naar hypothesen en visualisaties en vervolgens daarop aansturen is een nieuw vakgebied. De eerste successen op het gebied van fraudebestrijding, aantrekken van toeristen zijn gemaakt door respectievelijk de Belastingdienst en gemeente Rotterdam. Meer voorbeelden zijn te vinden op de [pilotstarter](#) van de VNG

De wens van gemeenten om regie te voeren, ingewikkelde wetgeving, veranderende taken en technische trends vragen van gemeenten een strakkere implementatie van de PDCA-cirkel (Plan-Do-Check-Act). Met name de “Check” fase (beleidsvalidatie) vraagt om overzicht. Bestuurders en directies hebben behoefte aan (management)Informatie om op te sturen en over te beslissen.

Door de komst van Big Data is het mogelijk real time een veelvoud van data te analyseren. Het stelt ons in staat om het effect van beleid vooraf te evalueren (beleidsbepaling). In zijn algemeenheid is er een trend om met big data en datamining (patroonherkenning) meer nadruk te leggen op preventie en innovatie dan op reparatie van beleid.

Doelstelling

- Doelstelling voor de gemeenten: per beleidsterrein en/of aandachtsgebied bepalen welke patronen er herkend moeten worden en hoe deze informatie kan worden gebruikt om (preventief) testuren.
- Doelstelling voor de WODV/ I&A: faciliteren, adviseren en implementeren van informatiesystemen, geschikt voor Big data toepassingen.

Richtlijnen

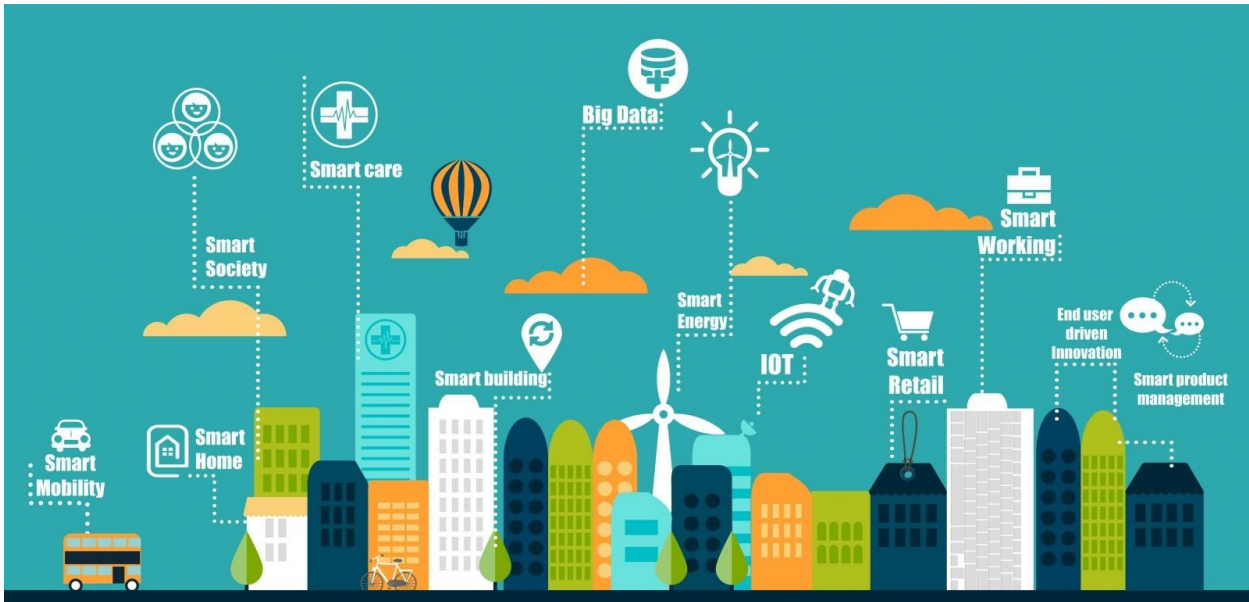
- De gemeenten investeren in Big-Data toepassingen waarbij de privacy van inwoners niet in het geding komt.
- De gemeenten investeren samen met de samenleving in een netwerk dat het mogelijk maakt om informatie van dingen (The Internet of things) te verzamelen. Denk aan informatie over inwoners in wijken en dorpen, over bijvoorbeeld gezondheid, vervoersvraagstukken. Deze gegevens zijn openbaar.
- Big Data-analyses worden op een gebruiksvriendelijke manier beschikbaar gesteld voor de organisatie ten behoeve van de beleidscyclus.

Consequenties

- De WODV borgt de Big-Data functie in de organisatie
- Managers van vakafdelingen worden voorgelicht over de mogelijkheden van Big-Data (bewustwording)
- Er worden enkele pilots uitgevoerd.

Smart City

Een slimme stad maakt gebruik van informatie- en communicatietechnologie (ICT) om de kwaliteit, de prestaties en de interactiviteit van de stedelijke diensten te verbeteren, de kosten en het verbruik van hulpbronnen te verminderen en om het contact tussen inwoners en overheid te verbeteren.



Door Smart-City-concepten is het mogelijk om vraagstukken rondom de stad te beantwoorden. Denk aan het aantrekken van toeristen.

Bij veel vraagstukken kunnen Smart-City concepten worden toegepast:

- Aantrekken en informeren van toeristen door op locatie gebaseerde communicatie (ibeacon).
- Langer zelfstandig wonen door het implementeren van een zorg-netwerk.
- Energiebesparing realiseren door intelligente lantaarnpalen.
- Klimaatneutraliteit bereiken door toepassing van slimme duurzame energievoorzieningen op gebouwen en publieke transportmiddelen.
- Vershraling van de winkelcentra tegengaan, de aanwezigheid van snel internet en beacons waardoor fysieke winkels de concept-store van de internetwinkel wordt (Smart Retail).
- Fietsen in de stad bevorderen door regensensoren op stoplichten te plaatsen, zodat fietsers tijdens een regenbui vaker voorrang krijgen (Rotterdam).

Doelstelling

- Doelstelling voor de gemeenten: ambities formuleren voor het toepassen van Smart-City functionaliteiten.
- Doelstelling voor de WODV/ I&A: faciliteren, adviseren en implementeren van informatiesystemen, geschikt voor Smart-City toepassingen.

Richtlijnen

- De gemeenten investeren samen met de ondernemers in Smart-City concepten (co-financiering)
- De WODV experimenteert met Smart-City toepassingen

Consequenties

- De WODV inventariseert de vragen waarvoor Smart-City toepassingen ingezet kunnen worden.
- De WODV prioriteert de vragen en maakt een business case voor de belangrijkste vraag
- De WODV gaat in gesprek met ondernemers om de business case uit te voeren.
- De WODV/I&A bouwt kennis op over Smart-City toepassingen

Hoe kan ik altijd en overal mijn werk doen?

Ambtenaar 3.0 is de ambtenaar die middenin de samenleving staat. Welke middelen heeft hij tot zijn beschikking om met inwoners en ondernemers te werken aan een betere samenleving? Hoe werkt hij aan actuele vraagstukken zoals in het sociaal domein en de omgevingswet? Welke digitale vaardigheden heeft hij daarbij nodig? En welke middelen?

Digitaal samenwerken, papierarm, intern en extern

De samenleving digitaliseert in hoog tempo, mede door de introductie van mobiele devices. De meeste medewerkers vergaderen al digitaal. Ook plaats- en tijdonafhankelijk werken en e-dienstverlening vereist dat steeds meer informatie digitaal beschikbaar is.

Veel gemeentelijke organisaties houden er een duaal stelsel op na: veel gaat nog op papier, ook omdat de buitenwereld (inwoners, ondernemers, maatschappelijke partners) nog papier blijft sturen, maar grote delen gaan ook al digitaal via e-formulieren, e-mail, pdf-bestanden, etc. De WODV werkt toe naar een substitutiebesluit om ook het archief volledig digitaal in te richten.

Doelstelling

- Doelstelling voor de gemeenten: maximaal digitaal werken
- Doelstelling voor de WODV/I&A: digitalisering en automatisering van werkprocessen

Richtlijnen

- Alle informatiestromen verlopen digitaal: 'pas toe of leg uit'
- Er is een duidelijke scheiding tussen privé-data en zakelijke data
- Apps en clouddiensten mogen binnen beveiligingsrichtlijnen onbeperkt gebruikt worden, zolang het geen formele archief plichtige gegevens betreft. Wel zijn er gemeentelijke standaarden of veel gebruikte toepassingen.
- Er is een systeem voor ongestructureerde informatie (documenten) die gebruikt wordt voor creatieve c.q. beleidsvormende processen, dat vanaf elke plek toegankelijk is
- Het is altijd duidelijk dat men met de laatste versie van informatie c.q. documenten werkt
- Medewerkers maken gebruik van kennissystemen.
- Binnen de informatiesystemen wordt "Google" achtig zoeken mogelijk.

Consequenties

- Alle werkprocessen worden geoptimaliseerd (lean) en dan gedigitaliseerd
- Medewerkers krijgen een cursus 'verbetering digivaardigheid'
- Advies voor standaard Apps opstellen en uitrollen naar medewerkers
- Invoering van een collaboration-tool voor het faciliteren van informatie-uitwisseling t.b.v. creatieve processen
- Alle klanten en ketenpartners sturen hun vraag en informatie digitaal
- Invoering van een sociaal intranet als kennissysteem (kan ook ingezet worden als collaboration tool)
- Er wordt samen met communicatie een communicatiecampagne gestart naar inwoners om digitaal communiceren te promoten, gecombineerd met het actief ontmoedigen van de papierstroom

Het Nieuwe Werken / Sociale innovatie

Binnen veel gemeentehuizen worden verbouwingen uitgevoerd en wordt een flexibel werkplekbeleid ingevoerd. Vaak ook worden er mobiele devices verstrekt (tablets, smartphones, laptops) zonder dat er eenduidigheid is over voorwaarden om deze te verstrekken. Veel gemeenten geven vanuit hun visie op bedrijfsvoering aan, dat medewerkers meer “employable, taakvolwassen en omgevingsbewust” moeten worden, wat o.a. bereikt wordt door het geven van noodzakelijk vertrouwen en vrijheid.

Bij vrijheid hoort ook dat er mogelijkheden zijn om plaats en tijdonafhankelijk te werken. Dit is o.a. ook nodig in het sociale domein voor het voeren van het “keukentafelgesprek”.

Een kanttekening bij deze ontwikkeling is dat bereikbaarheid, (informele) kennisuitwisseling tussen collega’s en kennis over beschikbaarheid steeds belangrijker wordt, om ervoor te zorgen dat de organisatie nog wel als organisatie blijft functioneren.

Doelstelling

- Doelstelling voor de WODV: interne sociale innovatie waardoor medewerkers productiever, creatiever, meer verbonden zijn
- Doelstelling voor de WODV/ I&A: faciliteren van sociale innovaties door inrichting van flexibele werkplekken, versterken van mobility, bereikbaarheid en inzicht in beschikbaarheid

Richtlijnen

- Iedereen heeft de mogelijkheid om zakelijk te werken met mobiele devices
- Medewerkers kunnen 24X7 uur werken, plaats en tijd onafhankelijk. Er wordt een adequate ondersteuning vanuit de I&A-organisatie geregeld
- Interne communicatie tussen medewerkers is snel, eenvoudig en persoonlijk
- Met behulp van een registratiesysteem is de beschikbaarheid en bereikbaarheid van medewerkers is bekend en optimaal geregeld
- Voor een deel van de medewerkers is ook de plaats waar ze zich bevinden bekend t.b.v. een snelle inzetbaarheid ter plaatse

Consequenties

- Alle agenda’s van alle medewerkers staan open en beschikbaarheid wordt aangegeven
- Medewerkers van de buitendienst zijn via Google maps traceerbaar
- Inloggen op de telefoon is verplicht om ook de beschikbaarheid van medewerkers te kunnen zien
- Unified messaging biedt de mogelijkheid om te communiceren met spraak, beeld en tekst
- Er wordt een systeem geïntroduceerd waarmee medewerkers de beschikbaarheid van collega’s kunnen checken
- Invoering van een collaboration-tool (Social Intranet, Viadesk, Sharepoint, All-fresco)
- Medewerkers én inwoners kunnen tijdens openingstijden werken/gebruiken in het gemeentehuis, maar ook bij samenwerkingspartners, openbare gebouwen, maatschappelijke partners, etc.

Applicatierationalisatie: werken onder architectuur

Jaarlijks gaat er veel budget op aan onderhoudskosten, licentiekosten etc. Landelijk ging in 2013 gemiddeld 29,5% van het ICT-budget op aan software (Benchmark ICT, 2015). Dit is exclusief beheerkosten. Bij elkaar zal ruim 1/3 van het jaarlijkse ICT-budget hieraan opgaan. Afhankelijk van lopende projecten kan dit percentage nog een stuk hoger liggen. Er wordt steeds kritischer naar ICT-budgetten gekeken, o.a. door de extra aandacht die ICT binnen de overheid de afgelopen jaren in de media heeft gekregen.

Door I&A in een vroeg stadium te (laten) betrekken, kan een wildgroei aan applicaties worden voorkomen. Regelmatig is de benodigde functionaliteit al wel in huis, maar is dat alleen niet overal bekend. Door objectief en kritisch te kijken naar het applicatielandschap en dubbelingen en onnodige applicaties te schrappen, kan in veel gevallen het applicatieportfolio verkleind worden. Ook KING geeft in de handreiking Basis op Orde aan dat “een consolidatie van wat er zonder regie gegroeid is in de informatievoorziening besparing kan opleveren”.

Bovenstaande besparing bestaat alleen uit de vervallen onderhoudskosten e.d. Echter, minder applicaties leidt ook tot

een afname van de behoefte aan (technisch en functioneel) applicatiebeheer. Daarnaast is bij een lager aantal applicaties ook een lager aantal servers en minder opslag nodig. Dit zorgt ook weer voor minder benodigd technisch beheer en minder licentiekosten.

De hierboven genoemde zaken zijn een wens van velen, maar wat is de weg er naartoe? Een belangrijke basisvoorwaarde is applicatieportfoliomanagement. Het is minimaal nodig om te weten welke applicaties er binnen de organisatie precies aanwezig zijn, door wie, hoe en waarom ze gebruikt worden. Op deze manier is een eerste schifting soms al te maken. Verbind vervolgens applicaties met bedrijfsprocessen en bepaal hiermee de waarde van de applicatie. Op deze manier wordt tegelijkertijd inzichtelijk welke applicaties er per proces gebruikt worden en andersom. Door een bedrijfsproces te ontdoen van onnodige en overlappende applicaties, kan naast een deel van de IT, het bedrijfsproces zelf ook gelijk meer lean gemaakt worden.

Soms zijn er inderdaad vakspecifieke functionaliteiten die het leven makkelijker maken. De afweging moet dan gemaakt worden of dit een applicatie noodzakelijk maakt of dat het werk ook op een generieke manier in een andere applicatie gedaan kan worden. Wegen de voordelen, bijv. ingebouwde wet- en regelgeving op tegen de kosten?

Op dit punt raken we ook de gebruikers van de applicaties. In principe is applicatierationalisatie iets wat het beste top-down en objectief uitgevoerd kan worden. Het uitfasen en/of vervangen van een applicatie raakt medewerkers echter direct bij hun werkzaamheden. Het is daarom belangrijk om de gebruikersgroepen goed te betrekken en mee te laten denken. Dit vermindert de weerstand.

Zeker nu meer en meer aandacht komt voor het buiten de deur zetten van applicaties of zelfs het gehele applicatielandschap, is het belangrijk om zo “schoon” mogelijk over te gaan. Door vooraf (soms harde) keuzes te maken om het applicatielandschap te ontdoen van onnodige en/of niet gebruikte applicaties, kan veel tijd en geld bespaard worden bij outsourcing.

Doelstellingen

- Doelstelling voor de WODV: het verlagen van de kwetsbaarheid en de kosten voor ICT
- Doelstelling voor de WODV/I&A: het verlagen van complexiteit binnen het applicatielandschap en limiteren van onnodige kosten

Richtlijnen

- De WODV/I&A zorgt met applicatieportfoliomanagement voor continu inzicht in applicaties en het gebruik ervan in bedrijfsprocessen
- Bij een wens voor een nieuwe applicatie wordt I&A tijdig betrokken en wordt eerst gekeken naar wat al beschikbaar is en wat daarmee de mogelijkheden zijn
- Bij de aanschaf van nieuwe applicaties wordt gekozen voor standaardfunctionaliteiten (dus in principe geen maatwerk). Er worden zo min mogelijk overlappende functionaliteiten gebruikt

Consequenties

- Een systeem voor applicatie portfoliomanagement wordt zo nodig aangeschaft en ingericht;
- I&A inventariseert alle applicaties die in de organisatie gebruikt worden;
- Een aantal applicaties kan mogelijk komen te vervallen, wat tijdelijk de werkzaamheden van medewerkers kan verstoren.

ICT-outsourcing

Outsourcing van de automatisering

Het wordt steeds prominenter: softwareleveranciers leveren steeds vaker hun applicaties vanuit de cloud. Zowel kern-applicaties (sociale zaken, servicebus, salarissen, burgerzaken) als de kantoorapplicaties (office, digitaal ondertekenen, presentaties). En het is ook begrijpelijk vanuit het standpunt van de leverancier: één gecontroleerde omgeving voor alle klanten. Elke gemeentelijke organisatie heeft thans al applicaties in de cloud en verkeert nu al in een hybride omgeving. Wat betekent dit voor de toekomstige ICT-functie? Deze vraag kan gesplitst worden in vier deelvragen:

- Wat betekent dit voor de automatisering en IT-beheer?
- Wat betekent dit voor het applicatielandschap en koppelingen?
- Wat betekent dit voor de personele bezetting?
- Hoe gaan we om met deze veranderingen?

Automatisering en IT-beheer

Het is overduidelijk dat wanneer veel applicaties in de cloud worden gezet, dat de automatisering in brokjes wordt ondergebracht bij de leverancier: de storage, servers en IT-beheer worden door de leverancier zelf geïmplementeerd c.q. uitgevoerd. Dit betekent dat we deze capaciteit niet meer zelf hoeven te organiseren, en dat het in-house serverpark steeds kleiner wordt. Wel zijn er interessante vragen te stellen als het gaat om beveiliging: voldoet de leverancier aan de richtlijnen van KING/VNG, Suwi, BRP, BAG, etc. Wat gebeurt er met de data als een bedrijf failliet gaat? Hoe is de back-up en de uitwijk geregeld?

Steeds meer organisaties kiezen voor cloud-oplossingen. Bekende voorbeelden zijn Office 365 en Google Docs, waarbij ook de mailserver naar buiten wordt verplaatst. Maar ook PinkRocade levert zijn iBurgerzaken-module alleen nog maar als een cloud-oplossing. Al deze ontwikkelingen leiden ertoe dat er minder apparatuur nodig is binnen de organisatie. Wel ontstaat er een grotere afhankelijkheid van betrouwbare en veilige netwerkverbindingen. Voor veel gemeenten is dit de belangrijkste reden om ook de automatisering uit te besteden. Dit kan zijn aan gespecialiseerde ondernemers maar ook aan shared service centra in een gemeenschappelijke regeling.

Applicatielandschap en koppelingen (informatisering)

Het applicatielandschap is in principe nog identiek, maar er is minder ruimte voor maatwerk. Het applicatielandschap zal in de toekomst een verzameling van applicaties zijn die bij verschillende leveranciers draaien. De vraag is dan meer hoe deze applicaties onderling (informatie-technisch) gekoppeld kunnen worden. Het belang van standaardisatie neemt dan alleen maar toe. Er wordt meer verwacht van de uitwisselbaarheid van gegevens.

I&A-medewerkers

De rol van I&A-medewerkers zal sterk veranderen. De traditionele beheertaken verminderen en maken plaats voor vakkundig adviseren aan de vakafdelingen. Operationeel worden er steeds meer taken naar buiten geplaatst. De servers en applicaties verdwijnen uit het kantoor. Intern is er steeds meer behoefte aan contractmanagement (SLA), het uitvoeren van (beveiliging)-audits en het slim inkopen van flexibele en schaalbare ICT-oplossingen. Ook de ICT servicedesk zal een andere vorm krijgen: deze is veel meer een doorgeefluik naar de applicatie-leveranciers. Dit vraagt om een majeure aanpassing aan de I&A-organisatie. Het gaat hier om ook veranderingen in competenties, kennis, kunde en ervaring.

Doelstellingen

- Doelstelling voor de WODV: beheersing kwetsbaarheid, continue kwaliteit, beheersing van kosten m.b.t. I&A.
- Doelstelling voor de I&A-afdeling: outsourcing van automatisering (eventueel in samenwerking met andere gemeenten), samenwerken met andere gemeenten op het terrein van informatisering.

Richtlijnen

- Medewerkers worden begeleid naar een nieuwe rol.
- Samenwerken op informatisering is geen must.
- Maak ICT-plannen niet meer voor 4 jaar maar korter.

Consequenties

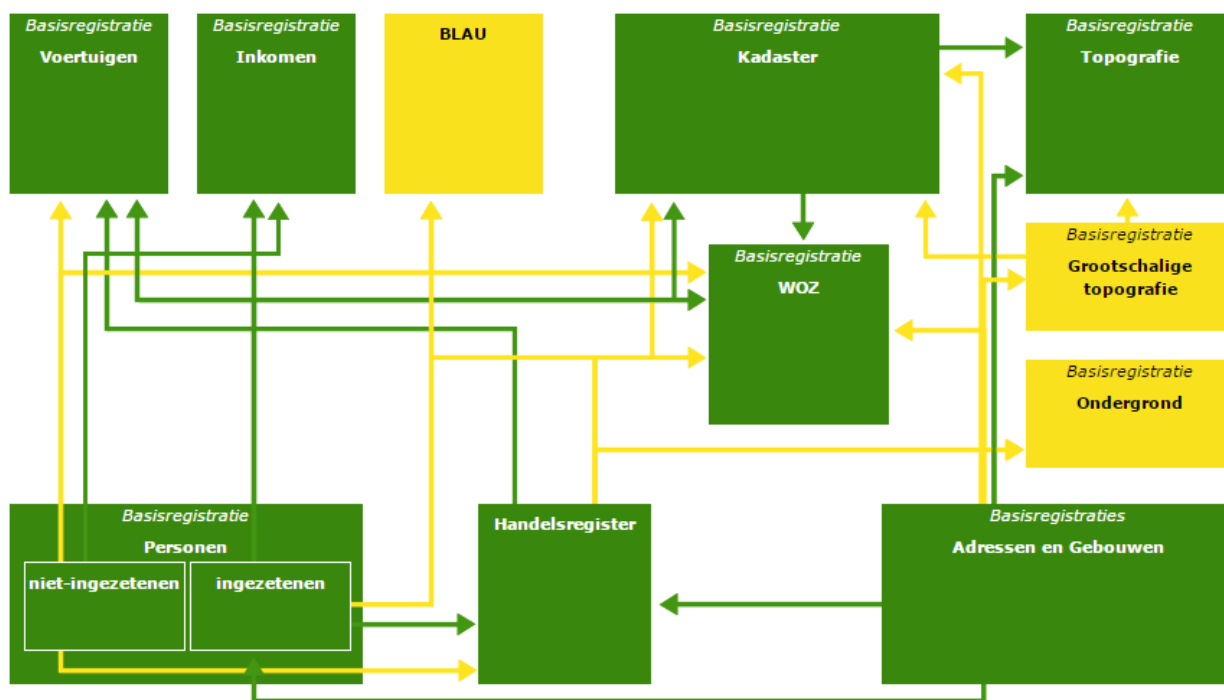
- Bepaal een outsourcing-strategie, mede gebaseerd op natuurlijke afschrijvingsmomenten.
- Herijk de visie jaarlijks en maak jaarplannen met acties en projecten.
- Neem medewerkers mee in de ontwikkeling: omscholen, kennis, kunde en ervaring opdoen.
- Zorg dat de ICT-infrastructuur en het licentiebeleid op orde zijn.
- Sluit contracten af voor een kortere tijd.
- Organiseer audits bij applicatie-leveranciers om de risico's van de cloud-oplossing te inventariseren.
- Start met marktconsultaties voor de uitbesteding van automatisering.
- Bepaal de strategie m.b.t. leveranciersbeleid: een vendor-lock creëert problemen. Zorg voor een exit-route.

De basis op orde

Gebruik van basis- en kerngegevens

Van de website van e-overheid.nl: “Het gebruik van het Stelsel van Basisregistraties heeft verschillende voordelen voor inwoners, ondernemers en afnemers. En om die voordelen zo groot mogelijk te maken, is het gebruik van het Stelsel van Basisregistraties gereguleerd in een wettelijk kader. Zo moeten 'bepaalde' organisaties in 'bepaalde' gevallen de authentieke gegevens uit de basisregistratie verplicht gebruiken en mogen deze gegevens in 'bepaalde' gevallen ook niet meer uitvragen bij burger of bedrijf. En in 'bepaalde' gevallen moeten zij bij gerede twijfel over de juistheid ook een terug-melding doen.”

Onderstaande afbeelding toont het stelsel van basisregistraties. De groene blokken zijn gerealiseerde basisregistraties. De gele blokken zijn de registraties die in de komende jaren ontwikkeld worden en waar gemeenten mee te maken krijgen:



De overheid wil dat de voordelen van het stelsel zo groot mogelijk zijn. Daarom is het gebruik van de gegevens uit het stelsel gereguleerd. Met ‘spelregels’ wordt gezorgd dat de gegevens in zoveel mogelijk processen worden gebruikt en dat de kwaliteit van de gegevens steeds beter wordt. De spelregels hebben de vorm van een wettelijk kader. Iedere basisregistratie heeft een eigen wet. Iedere van deze wetten beschrijft de volgende drie verplichtingen voor afnemers:

1. Niet meer uitvragen. Organisaties met een publieke taak mogen gegevens die beschikbaar zijn als authentiek gegeven niet meer uitvragen. Inwoners en ondernemers hoeven deze gegevens niet vaker aan te leveren dan nodig. Zo dalen de administratieve lasten.
2. Verplicht gebruik. Organisaties met een publieke taak gebruiken bij de vervulling van die taak gegevens. Zijn deze gegevens beschikbaar als authentiek gegeven, dan moet de organisatie ze afnemen van de basisregistratie.
3. Terugmelden. Bij gereede twijfel over de juistheid van een authentiek gegeven moeten afnemers daar melding van doen. De bronhouder zal dan onderzoeken of het gegeven nog wel juist is. Indien nodig wordt het gegeven bijgewerkt. Zo wordt de kwaliteit van de gegevens in de basisregistraties continu verbeterd.

De website e-overheid.nl biedt een leidraad om te bepalen welke werkprocessen te maken hebben met de basisregistraties.

Doelstelling

- Doelstelling voor de gemeenten: voldoen aan de wetgeving op de basisregistraties
- Doelstelling voor de WODV/I&A: minimaliseren van fouten en inconsequenties in basisgegevens

Richtlijnen

- Streven naar eenmalig vastleggen, meervoudig gebruik
- Voldoen aan de wet op de basisregistraties, en gekoppelde wetgevingen
- Er is één PDC voor producten voor inwoners en ondernemers
- Gebruik zoveel mogelijk landelijke standaarden voor informatieoverdracht zoals StUF, RSGB, RGBZ, NEN 3610, Digikoppeling en ZTC2.0
- Gebruik binnen de wettelijke regels bij alle communicatie het BSN nummer (voor zo ver dit binnen de privacyregels past)

Consequenties

- I&A implementeert de wet Generieke Digitale Infrastructuur
- I&A adviseert over het gebruik van de basisregistraties
- I&A koppelt geautomatiseerd of procesmatig de basisregistraties aan de vaktoepassingen

Informatie voldoende beveiligd

Gemeenten hebben zich in VNG-verband gecommitteerd om hoge prioriteit te geven aan informatiebeveiliging en om informatiebeveiliging bestuurlijk te verankeren. Tevens is afgesproken een gezamenlijk, gemeentebreed normenkader te hanteren, de Baseline Informatiebeveiliging Gemeenten (BIG).

Om tot een sluitend informatieveiligheidsbeleid op grond van de BIG te komen zijn de volgende stappen nodig:

1. Informatieveiligheidsbeleid opstellen: dit is het gemeentelijk beleid t.a.v. informatieveiligheid. Dit document dient bestuurlijk vastgesteld te worden. Informatieveiligheidsbeleid zal daarom in een separaat document ter vaststelling worden aangeboden aan het bestuur.
2. GAP-analyse uitvoeren: dit is het verschil bepalen tussen het in de BIG opgestelde normenkader en de feitelijke situatie.
3. Jaarlijks een risico-inventarisatie en -evaluatie (RI&E) uitvoeren. Hierbij wordt een rangorde opgesteld van de zaken die mogelijk de grootste bedreigingen vormen voor informatieveiligheid.
4. Opstellen dataclassificatie: Hierbij wordt een inventarisatie gemaakt van soorten informatie binnen de organisatie en het gewenste beveiligingsniveau.
5. Jaarlijks Informatiebeveiligingsplan (IBP): dit is een set concrete acties die uitgevoerd worden om het beleid stapsgewijs te implementeren. Het IBP is gebaseerd op de GAP-analyse, de RI&E en de dataclassificatie. Het IBP wordt jaarlijks ter vaststelling aangeboden aan het bestuur. In dit plan wordt bepaald wat er het komende jaar gedaan en geïmplementeerd gaat worden en tegen welke kosten.
6. Uitvoering van de maatregelen uit het informatiebeveiligingsplan en evaluatie van die maatregelen. Daarna begint de hier beschreven cyclus weer opnieuw (het informatiebeveiligingsbeleid dient gebaseerd te zijn op het Plan-Do-Check-Act principe). Bij deze cyclus worden sleutelfiguren op het gebied van ICT en gegevensbeheer uit alle domeinen van de organisatie betrokken.

Bij het opstellen van de informatiebeveiligingsrichtlijnen is de visie op bedrijfsvoering nog steeds van een groot belang: informatieveiligheid bestaat namelijk enerzijds uit harde technische acties, maar voor het belangrijkste gedeelte uit “zachte” maatregelen, gericht op de cultuur en de mensen in de organisatie. Het geven van vrijheid via digitale innovatie kan op gespannen voet staan met informatieveiligheid.

Doelstelling

- Doelstelling voor de gemeenten: informatiebeveiliging afgestemd op de visie op bedrijfsvoering en dienstverlening
- Doelstelling voor de WODV/ I&A: bouwen en implementeren van een inherent veilige informatievoorziening

Richtlijnen

- Onderschrijf de Baseline Informatieveiligheid Gemeenten.
- Beschikken over een actueel en integraal informatiebeveiligingsbeleid
- Zakelijke informatie is voor alle collega's toegankelijk, tenzij beveiliging of vertrouwelijkheid in het geding is.
- Hanteren van servicenormen voor het beheer van gegevens
- De vertrouwelijkheid en/of verlies van informatie is ALTIJD de verantwoordelijkheid van de gegevenseigenaar en de gebruiker, dus ook bij het gebruik van eigen devices of thuiswerkplekken.
- Er wordt gestreefd naar zo min mogelijk Informatiesystemen.

Consequenties

- Medewerkers worden geïnstrueerd over informatieveilig werken
- De WODV saneert het applicatielandschap via o.a. “werken onder architectuur”
- De WODV stelt een informatieveiligheidsbeleid op en laat dit vaststellen in het MT en bestuur
- De WODV stelt een informatiebeveiligingsplan op en laat dit vaststellen in het MT en bestuur
- Het informatiebeveiligingsplan dient uitgevoerd te worden. Hier zijn ongetwijfeld kosten aan verbonden.

Lean-IT: procesoptimalisatie binnen ICT

Gemeenten zijn grote informatie verwerkende organisaties. Je zou informatie als bouwstof kunnen zien voor gemeentelijke productieprocessen. Gemeenten verwerken informatiebouwstoffen, bewerken ze en creëren nieuwe informatie.

Gemeenten hebben de afgelopen jaren een behoorlijke slag gemaakt met procesoptimalisatie m.b.v. Lean. Kijk je naar informatiemanagement dan valt op dat daar sprake is van een achterstand met de toepassing van Lean. Juist door de beperkte zichtbaarheid en het gemak waarmee informatie kan worden geproduceerd, is kans op het ontstaan van verspillingen groot. Een aantal voorbeelden:

- Niet opgeschoonde netwerkschijven veroorzaken onnodig zoeken;
- Intranetten en kennissystemen bevatten vaak overbodige of dubbele informatie
- Dubbel ingevoerde klantgegevens;
- Onvolledige dossiers of klantgegevens die niet op een plek beschikbaar zijn;
- Schaduwadministraties in eigen sheets omdat informatie uit systemen niet wordt vertrouwd;
- Managementinformatie die niet juist blijkt te zijn en leidt tot handmatige telling.

Deze voorbeelden veroorzaken extra werk dat niet wenselijk is. Met een Lean-bril op, is er binnen de informatiewereld dus voldoende verbeterpotentieel. In de context van informatiemanagement zijn verliezen te omschrijven als alle extra activiteiten die ontstaan als gevolg van het niet voorzien van adequate, correcte en up-to-date informatie aan de eindgebruiker.

Gebruik het LEAN gedachtengoed om de kwaliteit van de informatievoorziening te analyseren. Niet slechts het infrastructurele aspect (datacenter, netwerk, werkplekken etc.) maar juist ook de informatieproducten, (rapportages, werklijsten, overzichten) de processen van gegevensinvoer of het doorgeven van informatie en de sturing op het gehele applicatielandschap.

IT-Verliezen	Voorbeeld	Lean-IT Strategie
Defecten en fouten	incidenten door ongeautoriseerde en ongeplande wijzigingen	Incident management
Over processing	De ontwikkeling van Applicaties en/of ICT diensten waarvoor geen klanten zijn	Portfolio management
Wachten	Slechte performance van applicaties Updates/onderhoud tijdens kantoor tijd	Performance management
Niet –waarde-toevoegend	Rapportages die niemand leest Controle omdat je je collega niet vertrouwt	Proces management
Transporteren	Afschuiven van problemen Verplaatsen/kopiëren van data	Proces redesign
Inventaris	Onduidelijk wat de werkvoorraad is, of welke “spullen” men in huis heeft	Asset management
Medewerkers onderbenut	Medewerkers zijn niet taakvolwassen en hebben te weinig kennis, maar krijgen ook niet de kans	HRM strategie
Extremen	Veel te hoge eisen aan de ICT-infrastructuur Te veel medewerkers	Demand management

Gezond boerenverstand en ICT

Het gevaar van informatiebeleidsdocumenten is dat deze maar al te vaak te globaal en te strategisch opgesteld worden. Om het informatiebeleidsplan scherpte te geven moet ook gedacht worden vanuit alledaagse gebruikersvragen en –problemen. Voorbeelden:

1. *Waarom moet ik gegevens dubbel invoeren in 2 systemen?*
2. *Hoe organiseer ik authenticatie: ik heb te veel systemen, gebruikersnamen en passwords?*
3. *Waarom zijn bepaalde processen zo bureaucratisch en vergen ze zoveel werk?*
4. *Waarom mag ik niet bij informatie op de fileserver en applicaties: wie mag er wel bij en wie niet?*
5. *Hoe kan ik makkelijker gegevens uitwisselen en verbinden in ketens, bv data van zorgverleners*
6. *Waarom kan ik niet mijn eigen apparaten gebruiken of kopen*
7. *Hoe weet ik of informatie relevant is als ik zoek (actueel, betrouwbaar, volledig)?*
8. *Wie is er eigenlijk eigenaar van systemen, data en processen binnen mijn organisatie?*
9. *Hoe zorg ik er voor dat collega's beschikbaar en bereikbaar zijn?*
10. *Kan ik niet-digivaardige collega's SLIM leren werken met ICT?*
11. *Hoe kan ik de licentiekosten drukken?*
12. *Hoe organiseer ik digitale informatie die ik krijg van collega's, partners, inwoners, etc.*
13. *Hoe krijg ik grip op koppelingen tussen systemen*

Voorbeelden veelvoorkomende spagaten:

- *We willen alle gegevens beschikbaar maar we schermen alles af vanwege informatiebeveiliging*
- *Medewerkers zijn taakvolwassen en resultaatgericht, maar we beschrijven hun werkprocessen tot in detail*
- *We willen vrijheid van werken en gebruik van allerlei systemen, maar de archiefwet vereist een NEN-gecertificeerd systeem*

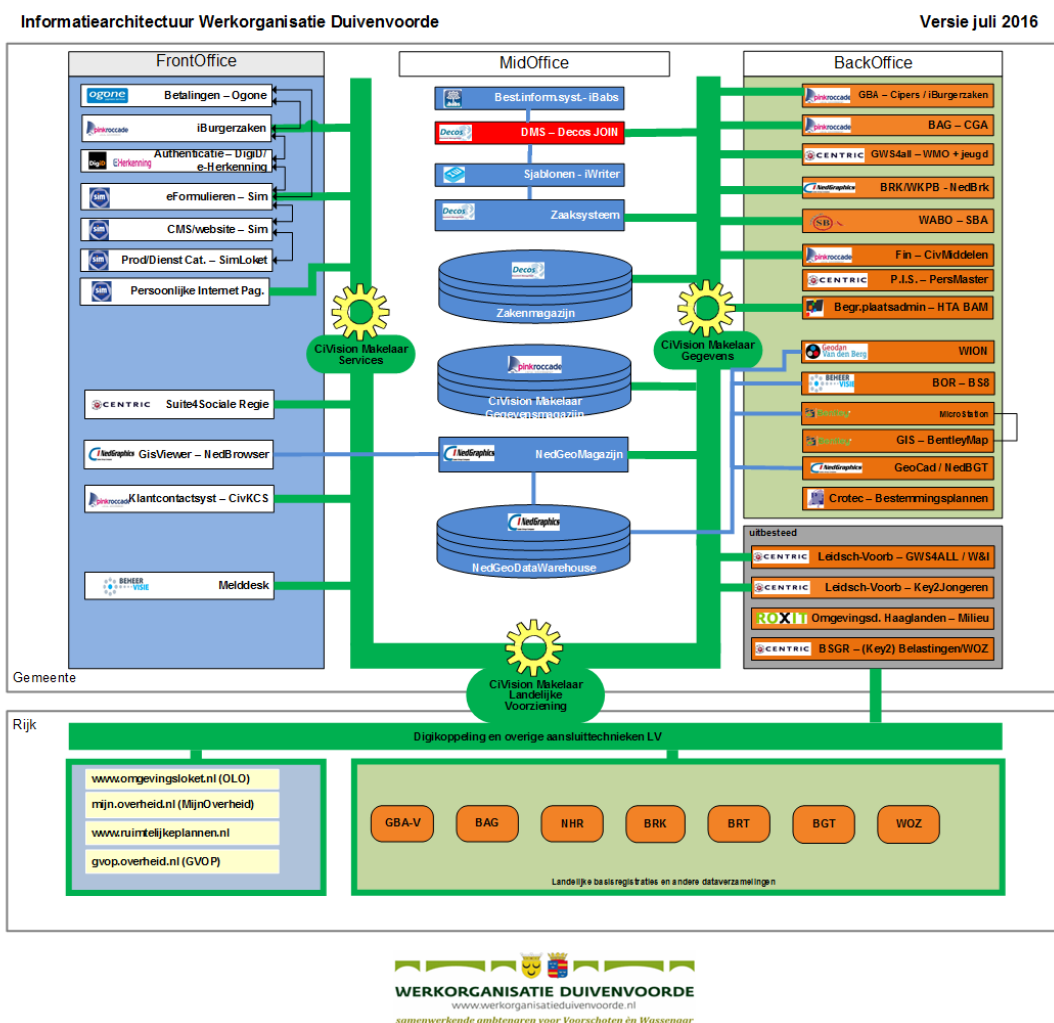
De I&A-architectuur visualiseert de ontwikkelopgave

Een visie op informatie en automatisering is mooi, maar is het praktisch en financieel haalbaar? Zijn er voldoende middelen? Kan de leverancier wel leveren? Is het wettelijk toegestaan? Is er voldoende kennis en kunde om e.e.a. te beheren? Daarnaast wordt de feitelijke implementatie sterk beïnvloed door de weging van de hier boven geformuleerde informatiebeleidsuitspraken. Wat weegt zwaarder? De kosten? Of dienstverlening? Of de flexibiliteit? Dit bepaalt in belangrijke mate de uiteindelijke implementatie.

Vanuit de bovengenoemde consequenties, die in elk hoofdstuk genoemd zijn, kun je kijken wat de impact is van de geplande activiteiten op de ICT infrastructuur, welk systeem of welke koppeling nodig is, etc. Daarvoor is het nodig om deze ict-infrastructuur eerst in beeld te brengen (IST) en van daaruit een schets te maken van

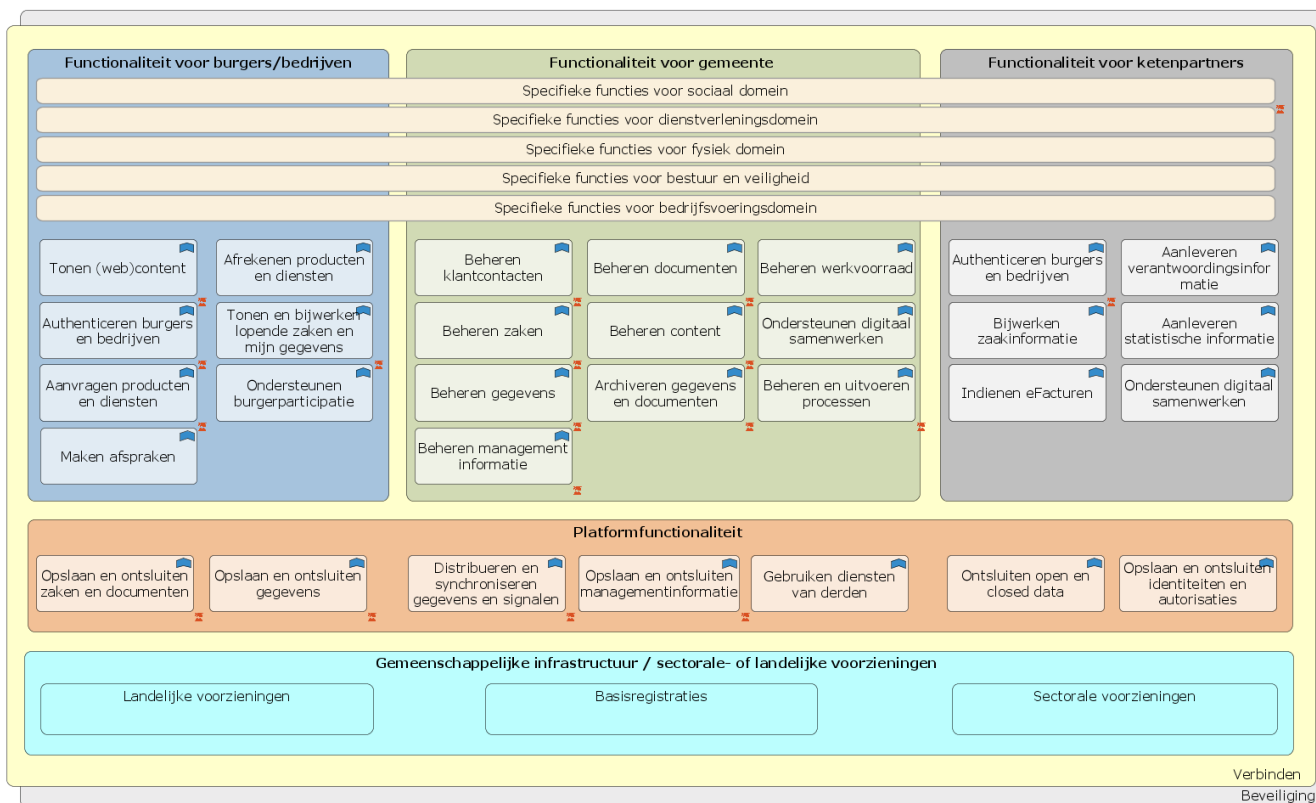
de toekomstige ICT in- frastructuur (SOLL).

Onderstaand de IST situatie van de Informatiearchitectuur van de Werkorganisatie Duivenvoorde, gebaseerd op de GEMMA referentie architectuur.



GEMMA 2

Eind 2016 is gestart met de ontwikkeling van een nieuwe GEMMA standaard. De GEMMA 2 informatiearchitectuur geeft een overzicht van de gemeentelijke applicatiefuncties. Het is een doorontwikkeling van de welbekende “Midoffice-plaat” en bijbehorende GEMMA Informatiearchitectuur 1.0 uit 2009. De GEMMA 2 Informatiearchitectuur is een referentiearchitectuur en is richtinggevend voor de inrichting van de informatiehuishouding van gemeenten. De plaat geeft een overzicht van gemeentelijke [applicatiefuncties](#) en ordent deze naar doelgroep en genericiteit. De informatiearchitectuurplaat kan gebruikt worden als basis voor een breed scala aan vraagstukken op het vlak van informatiemanagement en architectuur.



Hoe: de veranderopgave voor I&A-medewerkers en organisatie

Verandering is pas effectief wanneer medewerkers zich anders gedragen. Het aanpassen van systemen, het bedenken van nieuwe manieren van werken heeft pas nut wanneer ook de medewerkers handelen in lijn met de gestelde doelen. Medewerkers moeten enerzijds weten wat de bedoeling is en anderzijds worden betrokken bij keuzes die hen direct raken. De veranderopgave voor de gemeente is tweeledig: ten eerste liggen er concrete acties volgend uit het IBP die moeten worden doorgevoerd en ten tweede is er de zorg voor blijvende afstemming en 'fit' tussen organisatiedoelen en informatievoorziening.

Vergelijkbare trajecten laten zien dat er spanning kan ontstaan tussen het beheer van de bestaande ICT en de door te voeren veranderingen. Het duidelijk scheiden van de rollen beheer en ontwikkeling, het maken van goede afspraken over wijzigingsbeheer en een projectmatige aanpak kan vertraging voorkomen.

Het is belangrijk de aansturing van de veranderingen goed te borgen. Hiertoe dienen zowel opdrachtgever als opdrachtnemer van de verschillende acties te worden bepaald (zie onderstaande tabel). Het toewijzen van rollen aan personen vergroot de stuurbaarheid van de veranderingen.

Machts strategie	Planmatige strategie	Onderhandeling strategie	Programmatistische strategie	Interactieve strategie
13%	23%	18%	25%	21%
Doordruwen	Verhuizen	Onderhandelen	Trekken	Ontdekken
Sturing door top Doelgericht Legitieme macht Inbreng controllers Macht-dwang Geen participatie	Initiatief bij de top Doelgericht Expertmacht Inbreng adviseurs Rationeel-empirisch Weinig participatie	Meer partijen Resultaatgericht Positiemacht Inbreng partijen Onderhandeling Politiek proces	Participatief Probleemgericht Indirecte macht Inbreng medewerker Reëducatief Veel participatie	Interactief Toekomstgericht Verbeeldingskracht Samen optrekken Dialogo en conflict Veel interactie
Zeer laag Verander vermogen	Laag Verander vermogen	Gering Verander vermogen	Beperkt Verander vermogen	Hoog Verander vermogen

Kijkend naar de ambitie en reikwijdte van de in dit IBP gestelde doelen en acties is het van groot belang de besturing van de veranderopgave stevig vorm te geven. Hierbij werkt men het beste met programmasturing waarbij de rol van opdrachtgever wordt ingevuld door het directieteam.

De opdrachtnemer voor het programma, de programmamanager stuurt de projectleiders aan van de onder het programma vallende deelprojecten. Door projectleiders te selecteren, niet alleen vanuit de hoek van bedrijfsvoering, maar uit verschillende onderdelen van de organisatie wordt voorkomen dat het realiseren van het IBP een aangelegenheid van alleen bedrijfsvoering wordt.

Informatieveiligheid

Beleidsgrondslagen en -uitgangspunten



Versie 0.4, december 2016



**Gemeente
Voorschoten**

Gemeente



Wassenaar



WERKORGANISATIE DUIVENVOORDE

Inhoudsopgave

1	Managementsamenvatting	3
2	Inleiding	4
2.1	Het programma Digitaal 2017	4
2.2	Informatieveiligheid voor Digitaal 2017 een randvoorwaarde.....	4
2.3	VNG Resolutie Informatieveiligheid	5
2.4	Nieuwe technologie, nieuwe kwetsbaarheden	5
3	Informatieveiligheid	6
3.1	Wat is informatieveiligheid?	6
3.2	Waarom informatieveiligheid?	7
3.3	Gemeentebrede informatieveiligheid	7
4	Informatieveiligheidsbeleid	8
4.1	Doel van formuleren van informatieveiligheidsbeleid	8
4.2	Afbakening en reikwijdte informatieveiligheidsbeleid	8
4.2.1	Scope	8
4.2.2	Doelgroepen	9
4.2.3	Raakvlakken	9
4.3	Uitgangspunten voor informatieveiligheidsbeleid.....	9
4.4	Uitwerken van informatieveiligheidsbeleid.....	10
4.4.1	Beleidsdoelstellingen op hoofdlijnen.....	10
4.4.2	Uitwerking in jaarlijks informatiebeveiligingsplan.....	11
5	De organisatie van de informatiebeveiliging	13
5.1	Generieke verantwoordelijkheden in de informatiebeveiliging	14
5.2	Specifieke verantwoordelijkheden in de informatiebeveiliging	16

1 Managementsamenvatting

De overheid wil een betrouwbare partner zijn. Onze inwoners kunnen geen andere overheid kiezen en moeten er daarom op kunnen vertrouwen dat er uiterst zorgvuldig met hun (vertrouwelijke) gegevens wordt omgegaan.

Het functioneren van de overheid valt of staat met informatie. Of we nu onze rol als dienstverlener, handhaver, beheerder, control, management/ondersteuning, facilitair, ontwikkelaar of politiek orgaan vervullen, we kunnen niets zonder informatie en informatiesystemen.

Met de verder gaande digitalisering van de dienstverlening (o.a het programma Digitaal 2017) en talloze ontwikkelingen op technologisch gebied, nemen ook de risico's toe. Gegevens dienen beschermd te worden tegen inbreuken van buitenaf. Informatie moet veilig zijn.

Al met al is informatiebeveiliging geen vrijblijvendheid meer. Talloze incidenten, die mogen rekenen op uitgebreide aandacht van de pers, onderstrepen dit. Er wordt vanuit de politiek meer en meer ingezet om dit gebied ook bij gemeenten te professionaliseren: De Taskforce Bestuur en Informatieveiligheid Dienstverlening, die colleges rechtstreeks aansprak op hun verantwoordelijkheden rondom informatiebeveiliging, De VNG-resolutie die een zelfregulerend systeem vorm geeft, het oprichten van de Informatiebeveiligingsdienst Gemeenten (IBD), de Wet meldplicht datalekken, etc.

Was tot nu toe regelgeving op het gebied van informatiebeveiliging beperkt tot afzonderlijke domeinen zoals DigiD, Suwi-net, BRP, paspoorten en rijbewijzen en BAG, nu werken we toe naar een gemeentebrede informatieveiligheid. Keteninformatisering en het principe van enkelvoudige opslag en meervoudig gebruik, staat geen geïsoleerde benadering meer toe. Het nieuwe informatieveiligheidsbeleid is organisatiebreed en afdeling overstijgend. Informatieveiligheid moet opgenomen worden als normaal kwaliteitscriterium voor een gezonde bedrijfsvoering. Op den duur zou dit moeten leiden tot 1 audit voor alle informatieveiligheidsaspecten van de gemeente, dus een vermindering van de audit- last.

Het nieuwe, geïntegreerde beleid zal door gemeenten zelf moeten worden vastgesteld. De basis voor het beleid wordt immers gevormd door de in november 2013 aanvaarde VNG resolutie informatieveiligheid, niet door wetgeving. Om de gemeenten een richtlijn te bieden, is een normenkader ontwikkeld, de Baseline Informatiebeveiliging Gemeenten (BIG). Deze Baseline geeft niet alleen in ruim 300 maatregelen tot op detail aan wat voor gemeenten de norm is op het gebied van informatiebeveiliging, maar bevat ook een strategisch deel. In dit strategische deel wordt o.a. omschreven waar het informatieveiligheidsbeleid aan moet voldoen.

Deze notitie, die ter vaststelling zal worden aangeboden aan het dagelijks bestuur van de WODV, heeft tot doel om invulling te geven aan hetgeen in de strategische baseline wordt gevraagd om daarmee een lokaal vastgesteld raamwerk te bieden voor de verdere ontwikkeling en uitvoering van het informatieveiligheidsbeleid. Centraal in dit stuk staan doelen, grondslagen, uitgangspunten en randvoorwaarden van informatiebeveiliging en de organisatie en verantwoording over informatiebeveiliging. Dit beleid wordt éénmaal in de 4 jaar geëvalueerd, of zoveel eerder als nodig.

Nadere invulling van dit beleid door concrete maatregelen, wordt gedaan op basis van een ook door het Dagelijks bestuur van de WODV jaarlijks vast te stellen informatiebeveiligingsplan. Het informatiebeveiligingsplan komt tot stand op basis van inzicht in risico's en kritische bedrijfsprocessen, inzicht in het gewenste beveiligingsniveau van informatie (dataclassificatie) en een analyse van de verschillen tussen de norm (BIG) en de werkelijke stand van zaken (gap-analyse). Het informatiebeveiligingsplan bevat tevens een raming van de kosten van te nemen beveiligingsmaatregelen.

2 Inleiding

Dit document bevat beleidskaders voor informatiebeveiliging. De in dit document genoemde doelstellingen, uitgangspunten en randvoorwaarden hebben een sterk normerend karakter. Zij zijn gebaseerd op de Baseline Informatiebeveiliging Gemeenten, het normenkader voor informatiebeveiliging waaraan de gemeenten zich hebben gecommitteerd met het aannemen van de VNG resolutie inzake informatieveiligheid.

Met de richting die gegeven wordt in dit document kan verdere invulling geven worden aan het de beleid met concrete beveiligingsmaatregelen, die zullen worden beschreven in een jaarlijks **informatiebeveiligingsplan**.

Onderdeel van dit document is een beheerstructuur voor informatiebeveiliging, waarmee verantwoordelijkheden voor informatiebeveiliging worden belegd en informatiebeveiliging wordt ingebed in de reguliere planning- en control cyclus binnen de bedrijfsvoeringsprocessen.

De in dit document opgenomen richtlijnen gelden voor de gehele organisatie ("gemeentebreed"), voor alle processen en systemen.

2.1 Het programma Digitaal 2017

"Bedrijven en burgers kunnen uiterlijk in 2017 zaken die ze met de overheid doen digitaal afhandelen. Dus 's avonds na het werk makkelijk en snel vanaf de bank die gewenste parkeervergunning voor je nieuwe auto aanvragen of een terrasvergunning voor je café. Er komt een eenmalige gegevensuitvraag voor ondernemers die gebruik maken van het Ondernemingsdossier om bedrijfsgegevens uit te wisselen met de overheid. En zo zijn er nog vele voorbeelden te noemen van een veranderende manier van dienstverlening.

De overheid opereert als één: er is sprake van integrale dienstverlening, waarbij het niet uitmaakt bij welke overheidsorganisatie je als eerste aanklopt om alles wat komt kijken bij je verhuizing te regelen of je nieuwe bedrijf op te zetten. De overheid richt zijn processen in op de (dienstverlenings)vraag van burgers en bedrijven en voorkomt daarmee dat burgers en bedrijven steeds weer hun weg moeten vinden in het brede en complexe landschap van overheidsorganisaties. Ook stelt één overheid geen overbodige vragen meer en zorgt dat burgers en bedrijven met minder regels en procedures te maken krijgen.

Dat moet op zo'n manier gebeuren dat de dienstverlening aan burgers en bedrijven door de overheid verbetert, de informatie-uitwisseling sneller en makkelijker verloopt en de efficiëntie wordt verhoogd. Kortom, Digitale Overheid: betrouwbaar, veilig en betaalbaar"

Aldus de website van het Programma Digitaal 2017.

Om een compacte, efficiënte overheid te realiseren met hoogwaardige dienstverlening, is digitalisering een vereiste en is het digitale kanaal het voorkeurskanaal. Het uitgangspunt van het programma Digitaal 2017 is: digitaal waar het kan, persoonlijk waar het moet.

2.2 Informatieveiligheid voor Digitaal 2017 een randvoorwaarde

Zowel burgers als overheden werken veel digitaal en delen daarbij belangrijke gegevens. Daarom is het belangrijk dat overheden zorgvuldig met deze gegevens omgaan. Overheidssystemen moeten veilig zijn en weerstand kunnen bieden aan pogingen tot misbruik en aanvallen van binnen en buiten.

Voor alle betrokken overheidslagen (Rijk/ZBO's, provincies, gemeenten en waterschappen) is daarom een stelsel van verplichtende zelfregulering ontwikkeld. Het gaat er hierbij om dat informatieveiligheid onderdeel wordt van de reguliere bedrijfsprocessen. Voor elke overheidslaag is inmiddels een basismodel afgesproken voor informatiebeveiliging, de zogeheten baselines informatiebeveiliging. Voor de gemeenten gaat het hier om de Baseline Informatiebeveiliging Gemeenten, kortweg de BIG.

2.3 VNG Resolutie Informatieveiligheid

Om de acceptatie en implementatie van de BIG een bestuurlijke context te geven, is eind 2013 in de buitengewone algemene leden vergadering van de VNG de VNG resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" aangenomen. Met deze resolutie wordt vorm gegeven aan de afgesproken zelfregulering op informatieveiligheidsvlak. De Resolutie houdt onder meer in dat iedere gemeente het informatieveiligheidsbeleid vaststelt aan de hand van de BIG. Tevens zullen gemeenten informatieveiligheid zowel ambtelijk als bestuurlijk borgen en de invulling transparant maken voor burgers en bedrijven.

2.4 Nieuwe technologie, nieuwe kwetsbaarheden

De in Digitaal 2017 geformuleerde dienstverleningsambitie brengt ook nieuwe dreigingen en kwetsbaarheden met zich mee. Sommige bestaan uit risico's die we eerst ook wel liepen, maar waarvan de ernst toeneemt doordat het nu gaat om een grotere schaal waarop gegevens worden uitgewisseld. Een gemaakte fout in de gegevensverwerking heeft daardoor naar verwachting ook grotere gevolgen.

De technologische doorontwikkeling van de digitale internetdienstverlening, social media, cloudoplossingen, flexwerken, etc. brengt tegelijkertijd bedreigingen voor de informatieveiligheid met zich mee.

Denk aan de grootschalige inzet van mobile devices zoals smartphones en tablets, of het internet of things. Dergelijke apparaten bieden kansen op het gebied van bereikbaarheid, flexibiliteit en inzet op locatie, maar weten wij hoe adequaat te handelen in geval bijvoorbeeld een smartphone ergens 'vergeten' is of wellicht ontvreemd? Of als de sluis is gehackt?

Het gevaar wordt groter dat de informatie voor overheidsdienstverlening kan worden misbruikt of oneigenlijk kan worden gebruikt door kwaadwillenden en onbevoegden. Ook moeten organisaties steeds intensiever samenwerken om in staat te zijn de dienstverlening aan burgers en bedrijven op hoog niveau te verlenen. Dat betekent dat er steeds meer informatieketens ontstaan waarbij meer schakels dan alleen de gemeente betrokken zijn.

Een voorbeeld van een nieuw type risico is ook de toegenomen afhankelijkheid. Als alle dienstverlening digitaal gaat, zijn we ernstig onthand op het moment dat systemen weigeren of haperen. Om de dienstverleningsambitie waar te kunnen maken, is het hebben van een goede en betrouwbare infrastructuur cruciaal.

Dit alles maakt informatieveiligheid tot een complex vraagstuk. Een vraagstuk dat niet geïsoleerd vanuit de techniek of vanuit één domein bekeken kan worden. Het is allang niet meer zo dat informatieveiligheid als een technisch vraagstuk kan worden benaderd. Hoewel er wereldwijd een voortdurende technische wedloop gaande is tussen soft- en hardware fabrikanten en kwaadwillende hackers, schuilen de grootste risico's inmiddels in de gebruikers van informatie en de organisatie van informatieveiligheid. Sterker nog, behalve een technisch probleem, is informatieveiligheid nu ook een management probleem en kan razendsnel een bestuurlijk of zelfs politiek probleem worden.

e-Dienstverlening en informatieveiligheid staan soms op gespannen voet met elkaar!

3 Informatieveiligheid

3.1 Wat is informatieveiligheid?

Doel en proces

Informatieveiligheid en informatiebeveiliging

Informatiebeveiliging is dat wat je moet doen om informatieveiligheid te bereiken. Het doel moet niet zijn het verhogen van de informatiebeveiliging, maar het verhogen van de informatieveiligheid. Het middel hiervoor is informatiebeveiliging.

Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de kwaliteit van informatie te beschermen tegen al dan niet opzettelijk onheil.

Informatieveiligheid is het resultaat van dit proces, veilige informatie.

Kwaliteit en dataclassificatie

De kwaliteitsaspecten van informatie zien er zo uit:

beschikbaarheid / continuïteit	informatie is beschikbaar; staat voor de tijd waarin een informatiesysteem functioneert zoals bedoeld;
betrouwbaarheid / integriteit	informatie is juist, volledig, actueel en controleerbaar
vertrouwelijkheid / exclusiviteit	informatie is beschermd tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn (privacy)

In deze drie aspecten kunnen gradaties aangebracht worden, afhankelijk van het soort informatie. Niet alle informatie hoeft altijd voor de volle 100 % aan alle drie de aspecten te voldoen. Om te kunnen bepalen welke informatie in welke categorie valt, wordt een dataclassificatie opgesteld volgens het volgende model:

Niveau	Geen / 0	Laag / I	Midden / II	Hoog / III
beschikbaarheid	Niet nodig	Belangrijk	Noodzakelijk	Essentieel
betrouwbaarheid	Niet zeker	Beschermd	Hoog	Absoluut
vertrouwelijkheid	Openbaar	Bedrijfsvertrouwelijk	Vertrouwelijk	Geheim

Norm

Om te kunnen voldoen aan bovengenoemde kwaliteitseisen, moet informatie beveiligd zijn. Maar hoe weet je nou of de informatie voldoende beveiligd is? Het is in de praktijk lastig om het juiste beveiligingsniveau te bepalen.

Hiertoe is de Baseline Informatiebeveiliging Gemeenten opgesteld. De BIG vormt het normenkader waaraan informatiebeveiliging bij de gemeenten aan moet voldoen. De BIG is opgesteld door de door de VNG opgerichte Informatiebeveiligingsdienst Gemeenten en is afgeleid van internationale beveiligingsstandaarden ISO 27001 en 27002.

In de BIG zijn meer dan 300 beveiligingsmaatregelen opgenomen. Hiermee heeft de gemeente een instrument in handen waarmee zij kan meten of de organisatie "in control" is op het gebied van informatieveiligheid. Het is tot op zekere hoogte aan de gemeente om op basis van een risico inschatting te bepalen hoe zij prioriteert bij de invoering van de in de BIG opgenomen maatregelen en welke risico's zij aanvaardbaar acht.

Toets

Een centrale audit op het gebied van informatieveiligheid zal ontwikkeld worden. Vooralsnog zal deze audit bestaan naast de al bestaande audits op het gebied van BRP, Paspoorten en rijbewijzen, Suwinet, BAG en DigiD, uiteindelijk is de bedoeling dat de centrale audit in de plaats komt van de afzonderlijke audits, tenminste waar het betreft de informatieveiligheids aspecten.

3.2 Waarom informatieveiligheid?

In hoofdstuk 2 is het belang van informatieveiligheid aangegeven. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de werkorganisatie en de beide gemeenten. Het vormt de basis voor het beschermen van rechten van burgers en bedrijven.

Informatie is één van de belangrijkste bedrijfsmiddelen van een gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant is en proactief verantwoording aflegt aan burgers en raadsleden en die met minimale middelen maximale resultaten behaalt. De bescherming van waardevolle informatie is waar het uiteindelijk om gaat. Hoe waardevoller de informatie is en hoe groter de risico's zijn, hoe meer en hoe sneller maatregelen er getroffen moeten worden.

3.3 Gemeentebrede informatieveiligheid

Tot voor kort werd informatieveiligheid bij de gemeenten vooral benaderd vanuit de verschillende domeinen, zoals de Wet basisregistratie personen (BRP), de Paspoort- en rijbewijzen wetgeving, regelgeving omtrent het gebruik van Digi-D en regelgeving inzake Suwinet.

Op al die afzonderlijke gebieden bestaat uitgebreide regelgeving over beveiliging en privacy. Gezien de ontwikkelingen zal de focus van beveiligen echter moeten verschuiven: van het beveiligen van grote, nauwelijks verbonden, in eigen beheer zijnde data verzamelingen (bijv. BRP) naar dienstverleningsprocessen waarbij de data zich beweegt van de ene naar de andere dienstverleningspartner, of centraal binnen de organisatie of in de cloud is opgeslagen.

Hoewel op de afzonderlijke gebieden goede regelgeving bestaat, kunnen we gezien het bovenstaande met betrekking tot integratie en delen van data, tegenwoordig niet meer zonder een integrale benadering. Van een integrale benadering worden tevens efficiency voordelen verwacht: Waarom per domein in wetgeving vastleggen dat er een goede back-up gemaakt moet worden, als dat ook centraal geregeld kan worden? Waarom 3 à 4 keer een audit per domein als je met 1 audit kunt volstaan?

Inmiddels leert ook de sinds 1 januari opgedane ervaring met de Wet meldplicht datalekken dat beveiligingsrisico's zich veeleer voordoen in de periferie van de grote (basis)registraties, dan in deze registraties zelf. Een datalek ontstaat veel minder gauw in een op basis van sterk doorontwikkelde software gevoerde, met specifieke beveiligingswetgeving omkleedde basisregistratie, dan in de processen om dat soort registraties heen, zoals export van gegevens uit registraties d.m.v. een programma als excel, gegevens versturen via onbeveiligde mail, het kunnen inzien van persoonsgegevens via een onbeveiligde website applicatie, etc. Ook deze processen, die zich in de huidige, domein georiënteerde informatiebeveiliging aan het zicht onttrekken, zullen in beeld moeten komen om informatieveiligheid te kunnen bieden.

4 Informatieveiligheidsbeleid

4.1 Doel van formuleren van informatieveiligheidsbeleid

De Werkorganisatie Duivenvoorde wil inzetten op het verhogen van informatieveiligheid en verdere ontwikkeling van informatiebeveiliging in de organisatie. Ieder organisatieonderdeel is hierbij betrokken en dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. De WODV is zelf verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid.

Hierbij geldt:

- Los van wat de WODV zelf vaststelt, is er wetgeving waar altijd aan voldaan moet worden, zoals BRP, SUWI, DigiD, BAG en PUN, Archiefwet
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

Doel van het in deze notitie beschrijven van informatieveiligheidsbeleid en het laten vaststellen daarvan door het Dagelijks Bestuur, is om een beeld te schetsen van wat nodig is om informatieveiligheid te realiseren, richting te geven aan de verdere uitwerking in concrete maatregelen en verantwoordelijkheden duidelijk te maken.

Met het vastleggen van het beleid wordt tevens de eerste stap genomen om 'in control' te komen op het gebied van informatieveiligheid; wat willen we bereiken en welke maatregelen gaan we daartoe nemen. Implementatie wordt geborgd en toetsbaar en er wordt een beleidscyclus in gang gezet, waarover verantwoording afgelegd kan worden.

4.2 Afbakening en reikwijdte informatieveiligheidsbeleid

4.2.1 Scope

De scope van dit informatiebeveiligingsbeleid omvat de bedrijfsprocessen, onderliggende informatiesystemen en informatie van de WODV in de meest brede zin van het woord. Dit beleid is van toepassing op alle ruimten van alle in gebruik zijnde gebouwen, alsmede op de apparatuur die door werknemers gebruikt wordt bij de uitoefening van hun functie op diverse locaties. Dit beleid heeft betrekking op alle informatie die daarbinnen verwerkt wordt.

Ook als informatiesystemen niet fysiek binnen de werkorganisatie draaien is dit beleid van toepassing. Denk aan SAAS, cloud, uitbestede taken, etc.

Binnen de scope van dit beleid vallen alle op dit moment geldende normen en regels op het gebied van informatiebeveiliging die door derden aan gemeenten opgelegd zijn. Dit beleid bevat minimaal al deze maatregelen en brengt ze met elkaar in verband. Denk aan Baseline Informatiebeveiliging Gemeenten, Wet bescherming persoonsgegevens, Wet Basisregistratie Personen, Paspoorten- en rijbewijzenwetgeving, Suwinet en DigiD.

Informatiebeveiliging is méér dan ICT, computers en software. Informatiebeveiliging is een lijnverantwoordelijkheid en onderdeel van de kwaliteitszorg voor alle processen en de ondersteunende informatiesystemen.

Het gaat om alle uitingvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, netwerkcomponenten en andere hardware), maar vooral ook om mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral uit menselijk handelen en een tekort schietende organisatie. Verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.

4.2.2 Doelgroepen

Het gemeentelijk IB-beleid is bedoeld voor alle in- en externe medewerkers, zowel vast als tijdelijk, van de WODV, inclusief directie, dagelijks bestuur en algemeen bestuur en van de beide gemeenten (griffies, gemeentesecretarissen) alsook voor de beide gemeentebesturen.

4.2.3 Raakvlakken

Het informatieveiligheidsbeleid heeft raakvlakken met

- het *informatiebeleid*
- het *fysiek beveiligingsbeleid*
- de *informatiearchitectuur*
- het generieke *risico-management*

Deze beleidsvelden moeten op elkaar zijn afgestemd.

Op landelijk niveau worden de processen van informatiebeveiliging onderdeel van de volgende GEMMA versie om daarmee de basis voor ankering van informatieveiligheid in de bedrijfsvoering te verstevigen.

Tevens houdt dit in dat bij de inpassing van nieuw aan te schaffen software vanaf het begin van het aanschafproces/aanbestedingstraject aandacht wordt besteed aan informatieveiligheidsaspecten.

Hiertoe worden informatieveiligheidsaspecten opgenomen in de standaard ICT-aansluitvoorwaarden en in specifieke programma's van eisen.

Bijvoorbeeld: Software die zelfs de meest elementaire beveiligingscomponent als 'logging op gebruikersniveau' en een registratie hiervan mist, moet vermeden worden.

4.3 Uitgangspunten voor informatieveiligheidsbeleid

1. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met het Dagelijks Bestuur als eindverantwoordelijke. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2. Door periodieke controle, organisatie brede planning en coördinatie, wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid is afgestemd op informatiebeleid en fysiek beveiligingsbeleid en vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In zowel het informatiebeleid als het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Beide documenten worden periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en op te stellen risico- en gap-analyses.
3. Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.
4. De WODV en de beide gemeenten stellen de benodigde mensen en middelen beschikbaar om haar informatie te kunnen beveiligen op de manier gesteld in dit beleid.
5. Regels en procedures voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
6. Medewerkers, zowel vast als tijdelijk, intern of extern, worden geïnformeerd over het belang en gebruik van beveiligingsprocedures en zijn verplicht waar nodig gegevens en

informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

4.4 Uitwerken van informatieveiligheidsbeleid

Bovenstaande uitgangspunten vormen het raamwerk van het informatieveiligheidsbeleid van de Werkorganisatie Duivenvoorde. Dit dient nader uitgewerkt te worden.

4.4.1 Beleidsdoelstellingen op hoofdlijnen

Hetgeen in dit en voorgaande hoofdstukken is beschreven leidt op hoofdlijnen tot de volgende beleidsdoelstellingen:

1	De Werkorganisatie Duivenvoorde hanteert de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt voor de te stellen eisen op het gebied van informatiebeveiliging.
2	Het informatieveiligheidsbeleid wordt één keer per 4 jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld ¹ .
3	De aanpak van informatiebeveiliging is 'risk based'. De opzet, bestaan en eventueel werking van beheersmaatregelen om de risico's op aanvaardbaar niveau te houden wordt jaarlijks getoetst (Risicoinventarisatie en -evaluatie).
4	De beveiliging van informatie is gebaseerd op het gewenste kwaliteitsniveau van informatie. Hiertoe wordt een classificatie van data vastgesteld (dataclassificatie). Deze wordt één keer per 4 jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld.
5	Er vindt jaarlijks een toetsing plaats om kwetsbaarheden in de informatievoorziening te onderkennen en om de voortgang van informatiebeveiliging in vergelijking met het voorgaande jaar zichtbaar te maken (gap-analyse).
6	Jaarlijks wordt een informatiebeveiligingsplan opgesteld.
7	Tenminste 1 x per 3 jaar vindt een toetsing door een externe partij plaats op technische kwetsbaarheden (periodieke pen-test).
8	Informatieveiligheid en gegevensbescherming zijn een integraal onderdeel van de kwaliteit van de bedrijfsprocessen (integraal management).
9	Informatieveiligheid wordt expliciet meegenomen in de wijze waarop bedrijfsvoering en projecten worden uitgevoerd. Informatieveiligheid maakt bijvoorbeeld deel uit van het PJC-gesprek en van afdelings- en teamoverleg
10	Informatieveiligheid wordt vanaf de start van de voorbereiding van projecten (waaronder inkoop- en aanbestedingsprojecten) expliciet als onderwerp geadresseerd. Hiertoe worden

¹ In afwijking van de BIG, die 3 jaar voorschrijft, kiezen wij voor een periode van 4 jaar.

	bij de start van een project een beschrijving van gegevensstromen opgesteld en getoetst en voor zover relevant een risicoanalyse en privacy impact assessment uitgevoerd.
11	De Werkorganisatie Duivenvoorde voldoet aan bij Wet gestelde specifieke eisen op het gebied van privacy- en informatieveiligheid (Wet bescherming persoonsgegevens, DigiD, Wet Basisregistratie Personen, Paspoort- en Rijbewijzen, Suwinet, Archiefwet, BAG).
12	De Werkorganisatie Duivenvoorde stelt eisen op het gebied van privacy en informatieveiligheid aan samenwerkingspartners die werken met gegevens van de WODV en beide gemeenten, legt eisen vast en heeft inzicht in de mate waarin daaraan wordt voldaan (bewerkssovereenkomsten, regie).
13	De Werkorganisatie Duivenvoorde informeert de medewerkers over informatieveiligheid; de medewerkers zijn privacy- en beveiligingsbewust.
14	Voor iedere applicatie in gebruik binnen de werkorganisatie dient een beheerder en een gegevenseigenaar aangewezen te zijn. Hiervan wordt door team I&A een register bijgehouden.
15	Het informatieveiligheidsbeleid en het informatiebeveiligingsplan worden vastgesteld door het Dagelijks Bestuur van de Werkorganisatie Duivenvoorde.
16	Informatieveiligheid maakt expliciet deel uit van de portefeuille van één van de leden van de Dagelijks bestuur van de Werkorganisatie Duivenvoorde.
17	Werkorganisatie Duivenvoorde heeft een planning- en controlcyclus ingericht voor de activiteiten op het gebied van informatieveiligheid.
18	De stand van zaken op het gebied van informatieveiligheid wordt 3 x per jaar gerapporteerd aan het verantwoordelijke directielid bedrijfsvoering binnen de concern-directie en aan de voor informatieveiligheid verantwoordelijke portefeuillehouder in het Dagelijks Bestuur.
19	Aan de beide gemeenteraden wordt jaarlijks via het jaarverslag van de Werkorganisatie Duivenvoorde (<i>jaarrekening</i>) verantwoording afgelegd over informatieveiligheid.
20	De Werkorganisatie Duivenvoorde maakt de invulling van informatieveiligheid, zoveel als verantwoord is, transparant voor burgers, bedrijven en ketenpartners (bijv. via www.waarstaatjegemeente.nl).

4.4.2 Uitwerking in jaarlijks informatiebeveiligingsplan

Nadere invulling van dit beleid door concrete beveiligingsmaatregelen, wordt gedaan op basis van een door het Dagelijks bestuur van de WODV jaarlijks vast te stellen informatiebeveiligingsplan. Dit informatiebeveiligingsplan komt tot stand op basis van inzicht in risico's en kritische bedrijfsprocessen, inzicht in het gewenste beveiligingsniveau van informatie (dataclassificatie) en een analyse van de verschillen tussen de norm (BIG) en de werkelijke stand van zaken (gap-analyse). Het informatiebeveiligingsplan bevat zoveel mogelijk een raming van de kosten van de te nemen maatregelen.

Een nadere uitwerking van de norm wordt geboden door de Baseline Informatiebeveiliging Nederlandse Gemeenten. Doelstellingen worden geformuleerd en er staat in meer dan 300 concrete maatregelen beschreven waar aan voldaan moet worden. Al die maatregelen worden in deze beleidsnotitie niet herhaald; hier wordt volstaan met de doelstelling dat de BIG wordt gehanteerd als normenkader.

Dit met uitzondering van het hoofdstuk over de organisatie van de informatiebeveiliging. Dit gedeelte van de BIG is in deze notitie opgenomen omdat de BIG eist dat het vast te stellen beleid een onderdeel bevat over de organisatie van de beveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden.

Het in VNG verband overeengekomen normenkader is vastgelegd in de [Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten](#) en de [Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten](#).

5 De organisatie van de informatiebeveiliging

Taken op het gebied van informatiebeveiliging mogen niet worden opgehangen aan uitsluitend één functionaris of afdeling. Daarvoor zijn inmiddels teveel medewerkers op de een of andere manier en van uit verschillende disciplines met het verwerken van informatie bezig. Bestuur, management en medewerkers zijn allemaal betrokken bij het verwerken van informatie en dus mede verantwoordelijk voor de veiligheid van die informatie.

Aan de andere kant is het ook niet zo dat een organisatie van het formaat van de Werkorganisatie Duivenvoorde medewerkers in dienst heeft die zich full-time met informatiebeveiliging bezig houden, wellicht m.u.v. de informatiebeveiligingsfunctionaris (CISO).

De te onderscheiden taken, gebundeld in een rol, zijn onderdeel van een groter geheel aan taken of meerdere rollen, in één functie. Een voorbeeld:

- | | |
|---|---------|
| • Systeem-beheerder: | functie |
| • Technisch informatiebeveiligings beheerder: | rol |
| • Uitvoeren logging: | taak |

In de paragrafen 5.1 en 5.2 is aangegeven welke rollen en taken in de informatiebeveiliging zijn te onderscheiden en hoe de verantwoordelijkheden zijn belegd.

Paragraaf 5.2 beschrijft de meer generieke rollen in informatiebeveiliging; bestuur, management, beheerders en gebruikers, paragraaf 5.2 beschrijft de specifieke functies met rollen die direct te maken hebben met informatiebeveiliging.

Bevoegdheid tot aanwijzing

In sommige processen zijn de rollen in de informatiebeveiliging vastgelegd in de op het proces betrekking hebbende wetgeving. Bijvoorbeeld: De beveiligingsfunctionaris BRP wordt genoemd in de Wet Basisregistratie Persoonsgegevens (BRP). De beveiligingsfunctionaris reisdocumenten wordt genoemd in de Paspoort Uitvoeringsregeling Nederland (PUN). Deze wetten schrijven ook voor welke autoriteit de bevoegdheid heeft de betreffende rol toe te wijzen aan een functie of persoon. Voorbeeld: in het Reglement Rijbewijzen staat dat de beveiligingsfunctionaris rijbewijzen wordt benoemd door de Burgemeester.

Waar dit niet het geval is, omdat geen sprake is van wettelijk voorgeschreven functies, zal de organisatie zelf vast dienen te stellen wie de bevoegdheid heeft om een taak/rol toe te wijzen. Bij de werkorganisatie is de hiertoe gebruikelijke instantie afdelingshoofd of directie.

5.1 Generieke verantwoordelijkheden in de informatiebeveiliging

Algemeen Bestuur

Het Algemeen Bestuur van de Werkorganisatie Duivenvoorde bestaat uit de beide voltallige colleges van de gemeenten Voorschoten en Wassenaar. De voorzitter van het algemeen bestuur is de voorzitter van het Dagelijks Bestuur; jaarlijks afwisselend de burgemeester van Voorschoten of van Wassenaar.

Het Algemeen bestuur stelt de begroting en de rekening van de werkorganisatie vast en heeft t.a.v. informatieveiligheid een controlerende taak.

Dagelijks Bestuur

Het Dagelijks Bestuur van de Werkorganisatie Duivenvoorde bestaat uit vier leden, namelijk: de burgemeesters van Voorschoten en Wassenaar, een wethouder van Voorschoten en een wethouder van Wassenaar.

Het Dagelijks bestuur is t.a.v. informatieveiligheid verantwoordelijk voor het vaststellen van informatieveiligheidsbeleid en het informeren van het Algemeen Bestuur hierover, o.a. door informatieveiligheid expliciet te op te nemen in begroting en rekening. Eén van de leden van het Dagelijks Bestuur heeft informatieveiligheid in zijn portefeuille.

Het Dagelijks Bestuur waarborgt dat de informatiebeveiligingsdoelstellingen worden vastgesteld, dat ze voldoen aan de kaders zoals gesteld in de Baseline Informatiebeveiliging Gemeenten en zijn geïntegreerd in de planning - en control cyclus.

Concerndirectie

Aan het hoofd van de Werkorganisatie Duivenvoorde staat de Concerndirectie. De Concerndirectie bestaat uit de gemeentesecretarissen van Voorschoten en Wassenaar. De Concerndirectie staat het Algemeen Bestuur, het Dagelijks Bestuur en de voorzitter bij de uitoefening van hun taken terzijde en adviseert hen in die hoedanigheid over het informatieveiligheidsbeleid en rapporteert over de uitvoering daarvan.

Eén van de twee leden van de Concerndirectie is verantwoordelijk voor de portefeuille bedrijfsvoering; informatieveiligheid maakt hier deel van uit.

De concerndirectie is verantwoordelijk voor het vaststellen van operationele procedures en protocollen op het gebied van informatieveiligheid.

Afdelingshoofd / teamleider

Het afdelingshoofd en de teamleider zijn verantwoordelijk voor informatiebeveiliging bij het uitvoeren van activiteiten in processen behorende bij hun domein (algemene, integrale procesverantwoordelijkheid), óók waar het betreft informatieketens buiten de WODV, Voorschoten en Wassenaar ((gegevensuitwisseling met derden) en voor het ontwikkelen en handhaven van organisatorische en personele beveiligingsmaatregelen (procedures en protocollen).

Afdelingshoofden en teamleiders agenderen informatieveiligheid voor afdelings-/teamoverleg en voor PJC-gesprekken (personele jaar cyclus = functioneringsgesprek/beoordelingsgesprek).

Afdelingshoofden zijn vaak gegevenseigenaren.

Specifiek: Afdelingshoofd Personeel, Organisatie en Informatie (POI)

Het team I&A maakt deel uit van de afdeling POI. Het hoofd POI vertegenwoordigt het aspect informatieveiligheid in het management team. Het hoofd POI is verantwoordelijk voor het ontwerpen van en adviseren over informatieveiligheidsbeleid en uitvoeringsprocedures.

Fysieke beveiliging

Fysieke beveiliging is belegd bij het team Facilitaire Zaken. De teamleider Facilitaire Zaken is verantwoordelijk voor het opstellen van beveiligingsbeleid en de uitvoering van de beveiliging van percelen, panden en ruimtes.

Technische beveiliging

Informatietechnologie is ondersteunend aan bijna alle processen. De eisen die aan ICT voorzieningen gesteld worden zijn hierdoor ingrijpend en hebben invloed op de inrichting van het gehele ICT landschap. Het team I&A beveiligt het landschap met systeemtechnische- en beheersmaatregelen. Binnen het team I&A zijn een aantal specifieke rollen benoemd, zoals technisch beveiligingsbeheerder, uitwijkcoördinator en informatiebeveiligingsfunctionaris (CISO). Zie paragraaf 5.2.

Applicatiebeheerders en gegevenseigenaren

Applicatiebeheerders en gegevenseigenaren zijn verantwoordelijk voor de veilige, juiste en actuele verwerking van de gegevens binnen de applicatie, tussen applicaties en binnen de keten (gegevensuitwisseling met derden). In veel gevallen zijn de applicatiebeheerders t.a.v. de door hen beheerde applicatie tevens beheerder informatiebeveiliging; verantwoordelijk voor autorisaties, logging, monitoring, signalering van incidenten en voor het versiebeheer van hun applicatie (patches, releases).

Voor iedere applicatie in gebruik binnen de werkorganisatie dient een beheerder en een gegevenseigenaar aangewezen te zijn. Hiervan wordt door team I&A een register bijgehouden.

Eindgebruikers

NB. Alle bovengenoemde groepen vallen ook onder de groep eindgebruikers!

Eindgebruikers vormen met hun gedrag in de omgang met informatie een essentieel onderdeel van informatiebeveiliging. Zij zijn verantwoordelijk voor hun informatieveilig gedrag. Zij zijn verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

5.2 Specifieke verantwoordelijkheden in de informatiebeveiliging

Rol	Taak
Informatiebeveiligingsfunctionaris (CISO)	Opstellen van het informatiebeveiligingsbeleid Adviseren management bij ontwikkelen operationele procedures Adviseren omtrent concrete beveiligingsmaatregelen Monitoren beleidsuitvoering Organiseren onafhankelijke audits Rapporteert rechtstreeks aan conerndirectie
<i>Controller Informatiebeveiliging</i>	Toezicht op realisatie van het informatieveiligheidsbeleid
Beveiligingsfunctionaris reisdocumenten	Ziet toe op de naleving van de beveiligingsmaatregelen in de PUN
Beveiligingsfunctionaris rijbewijzen	Ziet toe op de naleving van de beveiligingsmaatregelen in het RR
Beveiligingsbeheerder BRP *	Ziet toe op de naleving van de beveiligingsmaatregelen in het Informatiebeveiligingsplan BRP en waarde-documenten.
Informatiebeheerder BRP *	Bepalen autorisatieniveau, bevorderen beveiligingsbewustzijn
Applicatiebeheerder BRP *	Uitvoeren autorisaties Bewaken juiste uitvoering procedures gebruik BRP
Systeembeheerder BRP *	Fysieke beveiliging van BRP Uitvoeren back-up en recovery
Overleggroep Informatiebeveiliging (ook voor BRP en waardedocumenten *)	totstandkoming van risicoinventarisatie en –analyse, dataclassificatie, adviseren over gap-analyse, afstemmen beleidsuitvoering binnen domein en gemeentebreed.
Technisch beheerder informatiebeveiliging	Is operationeel verantwoordelijk voor de beveiliging van netwerken, servers (en eventueel) applicaties. In die zin draagt hij zorg voor de optimale implementatie van de beveiligingsmaatregelen en -systemen en de juiste parameterinstellingen. Beheert specifiek op beveiliging gerichte componenten/software als firewall en anti-virus Logging en monitoring. Alertering en incidentopvolging Uitvoeren Back-up en recovery

Beheerder informatiebeveiliging (rol binnen de taak van applicatiebeheerder)	Beheert autorisaties binnen applicaties, i.c. stelt op aanvraag van verantwoordelijke lijnmanagers autorisaties aan medewerkers in. Logging en monitoring, signalering. Patching.
<i>Functionaris Gegevensbescherming WBP</i>	<i>O.g.v. Europese wetgeving verplicht per 25-5-2018 toezicht houden op privacy; inventarisaties van gegevensverwerkingen maken; meldingen van gegevensverwerkingen bijhouden; vragen en klachten van mensen binnen en buiten de organisatie afhandelen; interne regelingen ontwikkelen; adviseren over technologie en beveiliging (privacy by design); opstellen of aanpassen van een gedragscode melden datalekken bij de Autoriteit Persoonsgegevens</i>
Uitwijkcoördinator	Opstellen calamiteiten- en uitwijk plan Plannen en coördineren oefeningen Coördineren daadwerkelijke uitwijk

* als opgenomen in informatiebeveiligingsplan BRP en Waardedocumenten