



# Enterprise architectuur principes

Zorgregie- en declaratiesysteem Sociaal wijkteam Zwolle

## Inhoudsopgave

|   |                                         |    |
|---|-----------------------------------------|----|
| 1 | Dienstverlening                         | 2  |
| 2 | Samenwerking & coalities                | 3  |
| 3 | Vormgeving van de informatievoorziening | 5  |
| 4 | Data                                    | 7  |
| 5 | Digitale weerbaarheid en veiligheid     | 8  |
| 6 | Informatiebeheer                        | 10 |
| 7 | Privacy                                 | 11 |

# 1 Dienstverlening

*De informatievoorziening en dienstverlening van de gemeente Zwolle zijn vertrouwd, consistent, en gebundeld, ongeacht het beleidsterrein of de afdeling waar de inwoner of partner contact mee heeft.*

## Rationale:

- Onze digitale principes stellen dat we digitalisering inzetten om aan te sluiten bij de behoeften van mensen en niet van systemen. Bovendien is de dienstverlening van de gemeente Zwolle altijd gebaseerd op (het realiseren van) de opgaven van inwoners en bedrijven van de stad Zwolle. Voor inwoners en bedrijven is er maar één organisatie. De informatievoorziening moet daarom naadloos aansluiten op de belevingswereld van die inwoner.
- Verzorgen van de klanttevredenheid: Inwoners en bedrijven zien de gemeente niet als een verzameling losse afdelingen, maar als één geheel. Door als één organisatie te communiceren en te handelen, wordt de dienstverlening eenvoudiger, transparanter en betrouwbaarder. Dit verhoogt het vertrouwen en de tevredenheid.
- Gericht op interne efficiëntie: Wanneer afdelingen vanuit één gedeelde architectuur werken, worden dubbele processen, systemen en data-invoer voorkomen. Dit leidt tot lagere operationele kosten en een effectievere inzet van middelen en personeel. Het voorkomt dat dezelfde informatie op verschillende plekken wordt opgeslagen en voor de inwoner kunnen we eenduidiger communiceren.
- Versterking van de gemeentelijke identiteit en merk: Een consistente uitstraling en communicatie in alle beleidsterreinen, zowel digitaal als fysiek, versterkt de identiteit van de gemeente Zwolle. Het draagt bij aan een professioneel en betrouwbaar imago.

## Implicaties:

### 1. Bedrijfskundige implicaties:

- Cultuurverandering: Er is een niet veranderende focus nodig van een afdelingsgerichte aanpak naar een organisatiebrede focus waarin samenwerking en gedeelde verantwoordelijkheid centraal staan. Dit vraagt om leiderschap en bewustwording.
- Geïntegreerde processen: Werkprocessen moeten ontworpen zijn vanuit het perspectief van de inwoner, zodat er geen 'silo's' meer zijn. Dit betekent dat een aanvraag die meerdere beleidsterreinen raakt, niet door de inwoner bij elke afdeling opnieuw ingediend hoeft te worden.
- Door dit principe te hanteren is er ook een groei naar kanaalonafhankelijkheid waarbij een inwoner een proces via kanaal A start, deze via kanaal B moet kunnen afhandelen zonder opnieuw gegevens te hoeven aanleveren/invoeren.
- Eén klantbeeld: Het is noodzakelijk dat de gemeente een integraal, 360-graden klantbeeld kan opbouwen en inzien, ongeacht waar het contact met de inwoner plaatsvindt.
- Rekening houden met diversiteit: Onze gemeente houdt bij digitalisering proactief rekening met de diversiteit van inwoners. Ook in onze dienstverlening houden wij er rekening mee dat iedereen mee kan doen, ook al je minder digitaal vaardig bent. Bij het ontwerp van dienstverlening vragen wij ons af of deze inclusief zal zijn.

## 2. Informatie- en Data-implicaties:

- Centrale, authentieke bronnen: De systemen en processen moeten worden ingericht om data eenmalig, bij de bron, vast te leggen en vervolgens te hergebruiken in de hele organisatie.
- Standaardisatie van data: Definities en structuren van belangrijke gegevens, zoals persoonsgegevens of adresgegevens, moeten overal consistent zijn. Dit vereist het vaststellen en handhaven van het gemeentelijk gegevensmodel. Deze implicatie gaat dus over de consistentie van het datamodel in de gemeentelijke voorzieningen.

## 3. Applicatie- en Technologie-implicaties:

- Hergebruik van componenten en services: Applicaties moeten gebouwd worden met herbruikbare, modulaire componenten (API's of microservices) voor functionaliteiten zoals identificatie, betalingen of het inzien van gegevens. Dit voorkomt het 'from-scratch' bouwen van dezelfde functionaliteit door verschillende afdelingen.
- Geïntegreerd applicatielandschap: Het applicatielandschap moet ontworpen worden om de naadloze uitwisseling van data te faciliteren, bijvoorbeeld door middel van een integratieplatform (API-management). Dit betekent dat applicaties die voorheen op zichzelf stonden, nu met elkaar moeten kunnen 'praten'.
- Uniforme portalen en kanalen: De gemeente moet investeren in één herkenbare digitale ingang, die de inwoner toegang geeft tot alle diensten, ongeacht de achterliggende afdeling. De gemeente moet daarmee ook conformeren aan landelijke uitgangen, denk aan de Berichtenbox waar inmiddels bijna 300 gemeentes op zijn aangesloten.

## 2 Samenwerking & coalities

*De gemeente Zwolle ondersteunt de samenwerking met partners door middel van een vooraf vastgestelde architectuur. De informatievoorziening stelt herbruikbare producten en diensten beschikbaar via gestandaardiseerde kanalen. De mate van toegang, de uitwisseling van informatie en de te gebruiken technologie zijn afgestemd op de aard van de samenwerking en vastgelegd in een duidelijk, consistent kader.*

### Rationale:

De rationale voor dit architectuurprincipe is gebaseerd op de noodzaak om een evenwicht te vinden tussen openheid en controle.

- Voorkomen van wildgroei: Zonder duidelijke kaders kunnen samenwerkingen leiden tot een complex en onbeheersbaar landschap van processen en systemen. Dit principe voorkomt dat elke samenwerking leidt tot een aparte, op maat gemaakte oplossingen, wat kostbaar en inefficiënt is.
- Standaardisatie en consolidatie verstevigt de digitale weerbaarheid en veiligheid van de wederzijdse organisaties.
- Risicobeheersing: Het vooraf vaststellen van juridische en IT-kaders minimaliseert risico's op het gebied van gegevensbeveiliging, privacy en contractuele verplichtingen. Dit is essentieel voor elke overheidsorganisatie.
- Voorspelbaarheid en transparantie: Het maakt de kosten en gevolgen van een samenwerking voorspelbaar. Ketenpartners weten van tevoren wat de mogelijkheden en beperkingen zijn, wat leidt tot snellere en transparantere onderhandelingen.

- **Schaalbaarheid en efficiëntie:** Door samenwerkingen te baseren op herbruikbare, gestandaardiseerde IT componenten kan de gemeente snel nieuwe partners toevoegen en bestaande samenwerkingen schalen, zonder dat dit een grote architectonische impact heeft.

## **Implicaties:**

### **1. Bedrijfskundige implicaties:**

- **Definitie van samenwerkingsmodellen:** De gemeente moet verschillende, vooraf gedefinieerde samenwerkingsmodellen opstellen, variërend van "losse data-uitwisseling" tot "integrale proceskoppeling". Elk model heeft een bijbehorend juridisch en financieel kader.
- **Eén contactpunt voor ketenpartners:** Partners worden geleid naar één loket voor samenwerkingen, in plaats van te moeten onderhandelen met verschillende afdelingen. Dit verbetert de communicatie en versnelt het proces.
- **Governance-structuur:** Er is een duidelijke governance-structuur nodig om te bepalen welke samenwerkingen binnen de gedefinieerde kaders passen en welke een uitzondering vereisen.

### **2. Informatie- en Data-implicaties:**

- **Architectuur is leidend:** de architectuur repository laat ook ketens zien, bijvoorbeeld door middel van keten weergaves. De architectuur laat daarbij duidelijk zien welke afhankelijkheden er zijn.
- **Grip op applicatie behoeftes:** Er is van tevoren een duidelijk kader over welke ICT voorzieningen door de gemeente ter beschikking worden gesteld voor de partner of viceversa. Hiermee worden duidelijke grenzen gesteld over waar een ketenpartner gebruik van kan maken en wie eigenaarschap behoort.
- **API-First benadering:** De gemeente moet haar data en functionaliteiten primair beschikbaar stellen via gecontroleerde Application Programming Interfaces (API's). Deze API's dienen als de officiële toegangspoorten voor ketenpartners, met ingebouwde beveiliging en autorisatie.
- **Gedefinieerde datamodellen:** Er moeten duidelijke en gestandaardiseerde datamodellen zijn voor uitwisseling. Partners moeten zich conformeren aan deze modellen om data te kunnen uitwisselen, wat de integriteit en bruikbaarheid van de informatie waarborgt.
- **Er worden afspraken vastgelegd op welke manier voldaan wordt aan wetten zoals de Archiefwet en WOO.** Uiteindelijk is het de verantwoordelijkheid van de gemeente om te voldoen aan de archiefwet en WOO.
- **Omgang met informatiewetten:** De gemeente moet afgewogen keuzes maken over de omgang met informatie van andere gemeentes. De verantwoordelijkheden reiken vaak alleen tot de eigen organisatie terwijl data van ketens ook onder de informatiewetten vallen.

### 3. Applicatie- en Technologie-implicaties:

- API-managementplatform: De gemeente gebruikt een centraal platform voor het beheren, beveiligen en monitoren van alle externe API's. Dit platform fungeert als de toegangspoort tot de 'extended enterprise'.
- Component-gebaseerde architectuur: De interne systemen moeten gebouwd zijn met modulaire componenten. Dit maakt het mogelijk om specifieke componenten of 'diensten' beschikbaar te stellen aan partners via het API-platform, zonder de interne architectuur bloot te leggen.
- Beveiligings- en auditlogica: De technische infrastructuur moet ingebouwde mechanismen hebben voor authenticatie, autorisatie en logging om te voldoen aan juridische eisen en om de activiteiten van externe partners te kunnen auditeren.

## 3 Vormgeving van de informatievoorziening

*De informatievoorziening van de gemeente Zwolle is ontworpen en ingericht als een uniform, ketenbreed en interoperabel geheel, gebaseerd op het Common Ground gedachtegoed en conform de landelijke referentiearchitecturen en standaarden.*

### Rationale:

- De architectuur hoort wendbaarheid van de organisatie te faciliteren en de inzet van moderne technologische ontwikkelingen te ondersteunen. Daarvoor is het nodig om uniformiteit en interoperabiliteit in de informatievoorziening te creëren.
- Doelmatigheid als grondhouding: De informatievoorziening is doelmatig dat het waarde geeft aan de bedrijfsprocessen en dienstverlening. Bovendien is de informatievoorziening zo vormgegeven dat er geen onnodige dubbelingen in functionaliteit bestaan.
- Conformeren aan landelijke standaarden en beleidskeuzes: De referentiearchitecturen NORA en GEMMA worden gehanteerd als standaarden en geven hiermee grotendeels de informatievoorziening vorm. Beleidskeuzes en kaders op landelijk niveau, specifiek de keuze voor Common ground, de nationale digitalisering strategie en de digitale agenda 2028 van de VNG bieden kaders voor de vormgeving van de informatievoorziening. Zwolle conformeert zich aan deze standaarden. Door te conformeren aan gedeelde, landelijke standaarden wordt de complexiteit van het totale IT-landschap significant gereduceerd.
- Minimaliseren van complexiteit: De architectuur wordt uniform, en niet per afdeling of per project bedacht, wat voorkomt dat de IV bestaat uit een wirwar van maatwerk en datasilo's
- Faciliteren van ketensamenwerking: De gemeente is niet een op zichzelf staande organisatie. Het werkt samen met (talloze) ketenpartners en samenwerkingsverbanden. De informatievoorziening moet deze samenwerking mogelijk maken. Het garandeert ook dat data en diensten naadloos kunnen worden uitgewisseld met andere gemeenten en ketenpartners die dezelfde standaarden hanteren. Deze aanpak garandeert dat alle data en diensten consistent, eenduidig en uitwisselbaar zijn, zowel binnen de organisatie als met externe ketenpartners. Het hanteren van een uniforme ketenarchitectuur maakt snellere implementatie mogelijk, omdat er kan worden voortgebouwd op bestaande, beproefde oplossingen. De gemeente hoeft niet langer zelf het wiel uit te vinden en kan direct inzetten op de ontwikkeling van de eigen, unieke dienstverlening.
- Focus op wendbaarheid: de informatievoorziening moet faciliterend zijn aan een snel veranderende organisatie waarbij wetgeving, onze inwoners, politieke ontwikkelingen en organisatorische invloeden hand in hand gaan. De informatievoorziening mag de bottleneck

niet zijn om op te treden als sterke gemeente, maar ook technologische ontwikkelingen mogelijk maken en deze in het werkproces te gebruiken.

### **Implicaties:**

#### **1. Bedrijfskundige implicaties:**

- **Werken onder architectuur:** Zwolle werkt onder architectuur. De functie van architectuur moet volwassen zijn ingericht waardoor andere teams effectief gebruik kunnen maken van de gestelde architectuur en deze ook voor iedereen helder is. Architectuur is daarbij een verplichting waar iedereen zich aan conformeert.
- **Governance:** Er moet een duidelijke governance-structuur zijn die afdwingt dat nieuwe projecten en diensten voldoen aan de gestelde architectuurstandaarden. Afwijkingen moeten worden gemotiveerd en goedgekeurd.
- **Cultuurverandering:** Medewerkers en leidinggevenden moeten de toegevoegde waarde van landelijke standaarden omarmen en accepteren dat niet alles meer maatwerk kan zijn.

#### **2. Informatie- en Data-implicaties:**

- **Inzet op open source:** Zwolle kiest bewust voor open source en de principes en waarden van de common ground. Ook hanteert Zwolle een open source tenzij principe als het gaat om werkplek applicaties. Daarbij de focus verschuiven van betaalde applicaties naar open source varianten. De implicatie is een significante verschuiving in het applicatielandschap naar modulaire, open source software gericht op maximaal hergebruik en het maken van combinaties van apps in plaats van systemen naast elkaar.
- **Centrale bronnen:** Data wordt niet meer in applicaties opgeslagen, maar in authentieke, centrale bronnen. Applicaties consumeren de data via standaard verbindingen. Dit is het kernidee van Common Ground.
- **Standaardisatie:** Alle data, processen en services moeten voldoen aan landelijke standaarden.

#### **3. Applicatie- en Technologie-implicaties:**

- **Ontkoppeld applicatielandschap:** De applicaties van de gemeente zijn niet langer monolithisch, maar ontkoppeld. Ze bestaan uit modulaire, herbruikbare bouwblokken die via gestandaardiseerde interfaces (API's) met elkaar communiceren.
- **Focus op data-infrastructuur:** De gemeente investeert in een robuuste data-infrastructuur die het beheren en ontsluiten van gegevens uit centrale bronnen mogelijk maakt.
- **Uitfasen van legacy:** Er is een plan nodig om legacy-systemen die niet voldoen aan de gestelde architectuur, gefaseerd uit te faseren en te vervangen door nieuwe oplossingen die wel compatibel zijn met de architectuur. Een belangrijk onderdeel hiervan is het veilig stellen (migreren, converteren) of gecontroleerd vernietigen van de inhoud van het systeem.

## 4 Data

*De gemeente Zwolle hanteert een datacentrische architectuur waarin data wordt beschouwd als een strategisch bezit die wordt beheerd en benut gedurende de gehele levenscyclus. De informatievoorziening is ontworpen om de juiste data met de juiste kwaliteit, van de bron van registratie tot de ondersteuning van strategische besluitvorming, beschikbaar te maken.*

### Rationale:

- **Integrale waardecreatie:** De waarde van data begint niet pas bij een dashboard; het begint bij de correcte en tijdige registratie. Dit principe garandeert dat investeringen in data niet beperkt blijven tot Business Intelligence-tools, maar zich uitstrekken over de hele keten, wat de totale waarde van de data verhoogt.
- **Enkelvoudige waarheid (Single Source of Truth):** Door de nadruk te leggen op de bron van registratie, wordt voorkomen dat er meerdere, conflicterende versies van dezelfde data ontstaan. Dit bevordert consistentie en betrouwbaarheid, wat cruciaal is voor zowel operationele processen als voor strategische analyses.
- **Verbeterde besluitvorming:** Beslissingen, zowel tactisch als strategisch, zijn alleen effectief als ze gebaseerd zijn op betrouwbare en actuele informatie. Door de data in de juiste context te plaatsen, wordt het mogelijk om van 'business intelligence' over te stappen naar daadwerkelijk 'databewust werken', waarbij data niet alleen feiten toont, maar ook helpt bij het begrijpen van trends en de oorzaak van problemen. We gebruiken data om nieuwe inzichten op te doen, betere keuzes te maken en innovatie te ondersteunen (principekaart).
- **Betere datakwaliteit en -integratie:** Door data centraal te beheren en te delen vanuit een "single source of truth", wordt de kwaliteit van de data verhoogd. Medewerkers hebben toegang tot eenduidige, actuele informatie, wat de besluitvorming verbetert. Inwoners kunnen de gemeente vertrouwen met data omdat we hier verantwoordelijk en integer mee om gaan. (principekaart).

### Implicaties:

#### 1. Bedrijfskundige implicaties:

- **Kwaliteitsstandaard voor data:** De architectuur garandeert dat data eenduidig, actueel en contextrijk is voor zowel transactionele doeleinden als voor datagedreven inzichten.
- **Datamanagement als motor:** de datamanagement functie fungeert als de centrale motor en als 'goed huisvader' waakt hij over de data. Daarmee worden zaken als data eigenaarschap en data kwaliteit afgedwongen. Langs de lijn van datamanagement worden standaarden afgedwongen en problemen rondom data en datakwaliteit gemonitord.
- **Data governance:** Er is een sterke governance-structuur nodig die eigenaarschap, verantwoordelijkheden en standaarden voor data vastlegt gedurende de gehele levenscyclus. Dit omvat onder meer beleid voor data-invoer, -kwaliteit en -archivering.
- **Cultuurverandering:** Medewerkers moeten bewust worden gemaakt van hun rol als 'dataregistranten' en 'datagebruikers'. De organisatiecultuur moet evolueren van 'ik verzamel data voor mijn taak' naar 'ik verzamel data als strategisch bezit voor de hele organisatie'.
- **Verantwoord omgaan met data:** conform de principekaart zijn we kritisch over welke data we delen met commerciële partijen. We verzamelen niet meer gegevens dan nodig en daar waar mogelijk geven we inwoners zelf controle over hun data.
- **Data en samenwerking:** als gemeente zijn wij ons bewust welke data wij zelf registreren en (onder juridische afspraken) delen met partners. Ook zijn wij ons bewust welke data wij verwerven door partners, en behandelen wij deze als goed huisvader op een juiste en integere manier.

## 2. Informatie- en Data-implicaties:

Common Ground-gedachte: Dit principe is een verlengstuk van het Common Groundgedachtegoed, waarbij data niet in applicaties wordt opgeslagen, maar op één plek wordt beheerd en vervolgens wordt ontsloten voor verschillende doeleinden (transactioneel, operationeel, analytisch). De omgang met data verschuift van dubbel opslaan en verwerken naar verwerken rechtstreeks vanuit de bron.

## 3. Metadata Management:

Alle data, van de bron tot aan het gebruik in een rapport, moet voorzien zijn van rijke metadata. Dit omvat informatie over de herkomst, definitie, actualiteit en betrouwbaarheid van de gegevens.

## 4. Applicatie- en Technologie-implicaties:

Ontkoppeling van data en applicaties: De architectuur moet een scheiding zichtbaar maken tussen de systemen die data registreren (bronsystemen) en de systemen die data gebruiken (applicaties, BI-tools, et cetera). Dit wordt gerealiseerd door data toegankelijk te maken via gestandaardiseerde API's.

## 5. Investerings in data-infrastructuur:

De gemeente moet investeren in een robuuste data-infrastructuur, waaronder een dataplatform en datamanagement-tools, die de verwerking, transformatie en ontsluiting van gegevens mogelijk maken over de gehele levenscyclus.

# 5 Digitale weerbaarheid en veiligheid

*De gemeente Zwolle borgt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie door informatiebeveiliging als integraal onderdeel van de informatievoorziening te ontwerpen. Daarmee houdt zij rekening met de betrouwbaarheid van de informatie binnen de processen van de gemeente, onderdeel hiervan is de classificatie en gevoeligheid van informatie. Deze aanpak is bij wijziging van de informatievoorziening niet een toevoeging achteraf, maar een fundamentele waarde die de architectuur in staat stelt om proactief ('by design') weerbaar te zijn tegen zowel externe dreigingen als interne risico's.*

### Rationale:

- Security by design: Door beveiliging vanaf de start in te bouwen, wordt de architectuur van nature robuust. Door vooraf de risico's op inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid in kaart te brengen kunnen passende maatregelen direct worden geïmplementeerd. Dit is effectiever en veiliger dan het toevoegen van beveiligingslagen aan reeds kwetsbare systemen.
- Voldoen aan normen: De architectuur wordt ontworpen om te voldoen aan de normen die in de BIO2 op basis van de Cybersecuritywet (Cbw) aan de gemeente wordt gesteld. Naar gelang het dreigingsniveau en te beschermen belangen kunnen verzwaarde maatregelen worden toegevoegd.
- Bescherming van publieke waarden: De gemeente beheert gevoelige data van inwoners en bedrijven en voert processen uit die van vitaal belang zijn voor de samenleving, waarbij een verstoring van cyberveiligheid kan leiden tot ernstige gevolgen voor de samenleving of de economie.
- Robuuste informatiebeveiligingsmaatregelen in de startarchitectuur, continue (kwaliteits-)verbetering, reactieve maatregelen voor detectie en het reageren op incidenten en calamiteiten zorgen ervoor dat de processen zelf en de informatie binnen de processen

systematisch worden beschermd tegen datalekken, ongeoorloofde toegang en verstoringen, wat het vertrouwen in de overheid versterkt en de processen van vitaal belang gecontinueerd houden.

- Kosten- en tijdsefficiëntie: Het is veel efficiënter en goedkoper om beveiligingsmaatregelen in de ontwerpfase mee te nemen dan om deze naderhand nog in te bouwen en eventuele schade na een incident te herstellen. Dit principe verlaagt de operationele kosten op de lange termijn.

## **Implicaties:**

### **1. Organisatorische implicaties:**

- Risicogestuurd denken: De verantwoordelijkheid voor beveiliging ligt primair bij de proces- en dataeigenaar. Door proces- en dataeigenaar bewust te maken van de risico's van dataonveiligheid binnen de processen, worden maatregelen afgewogen tegen het bedrijfsbelang en stimuleert dit de integrale aanpak binnen de bedrijfsprocessen en besluitvorming.
- Het integrale kwaliteitsmanagementsysteem voor informatiebeveiliging, privacy en informatiebeheer waarborgt de verbetercyclus (pdca) ten aanzien van het bestand zijn tegen nieuwe dreigingen, voorkomen van kwetsbaarheden en het blijvend voldoen aan wet- en regelgeving. De reactieve maatregelen borgen een snelle detectie van incidenten en calamiteiten, zodat de verstoring van de bedrijfsvoering zo klein mogelijk is.
- Training en bewustzijn: Medewerkers moeten voortdurend worden getraind om veiligheidsrisico's te herkennen en te voorkomen. Periodiek wordt het trainingsprogramma voor de medewerkers afgestemd op de actuele dreigingen. Gebruikersinstructies worden indien noodzakelijk hierop aangepast.
- Blijvende informatieveiligheid: Het beschermen van de integriteit, beschikbaarheid en vertrouwelijkheid van informatie gebeurt niet op één moment, maar gedurende de gehele levenscyclus van de informatievoorziening. De proces- en dataeigenaar ziet toe op het actueel houden van de risicobeoordeling en implementatie van het passende beveiligingsniveau.

### **2. Technologische implicaties:**

- Zero-Trust architectuur: Elk verzoek om toegang tot data en systemen wordt hiermee in beginsel altijd als onbetrouwbaar beschouwd en moet expliciet worden geverifieerd, ongeacht de locatie of gebruiker.
- Toegang is altijd persoonsgebonden, expliciet en procesgericht: Toegang tot gemeentelijke systemen gebeurt via een gestandaardiseerd proces waarbij vooraf is nagedacht wie toegang tot welke gegevens en functionaliteit krijgt waarbij de principes van 'need to know' en 'least privilege' wordt gehanteerd. Dit proces is op elk moment te monitoren. Dit vindt gestructureerd en periodiek plaats aan de hand van het Logische toegangsbeleid en op basis van autorisatie- en bevoegdheden matrices die door de eigenaren en beheerders per applicatie opgesteld zijn
- Koppelingen en informatiedeling: Koppelingen voorzien in het transport van data van- en naar applicaties. Zwolle hanteert een API tenzij uitgangspunt. In het geval bijzondere of gevoelige (persoons)gegevens via de koppeling uitgewisseld worden, moet een verzwaarde beveiliging van de koppeling worden ingeregeld.
- Logging en monitoring: De architectuur moet het mogelijk maken om alle activiteiten te loggen en te monitoren. Voor de monitoring worden usecases ontworpen met en door het Security Operation Center (SOC) op basis van voorziene risico's. Voor de usecases worden tevens runbooks ontwikkeld om snel te kunnen acteren op gedetecteerde afwijkingen. Hierdoor wordt afwijkend gedrag gedetecteerd, vindt analyse plaats en kan een passende

reactie op de dreiging worden ondernomen.. Ook wordt voorzien in een audittrail, waardoor herleid kan worden vanwaar de dreiging afkomstig is (geweest).

## 6 Informatiebeheer

*De gemeente beschouwt zowel data als documenten als publiek goed. Data en documenten worden als publiek goed beheerd en proactief transparant gemaakt. De gemeente hanteert het DUTO raamwerk als uitgangspunt voor het informatiebeheer.*

### Rationale:

- Betrouwbaarheid vanaf de bron: De kwaliteit van informatiebeheer staat of valt met de registratie en het beheer vanaf het allereerste moment. Door de focus op de creatiefase wordt voorkomen dat informatie later onbruikbaar of onbetrouwbaar blijkt te zijn, wat essentieel is voor juridische audits en verantwoording.
- Fundament voor datagedreven werken: Goed beheerde data en documenten vormen de basis voor inzichten en analyses. Dit principe is de onmisbare schakel tussen het principe van 'Datagedreven van bron tot besluit' en de realiteit van informatiecreatie in de organisatie.
- Naleving van wet- en regelgeving: Een proactief en gestructureerd beheer van informatie is de meest effectieve en efficiënte manier om te voldoen aan de eisen van de archiefwet, de Wet open overheid (Woo) en andere relevante wetgeving.

### Implicaties:

#### 1. Bedrijfskundige implicaties:

- Geïntegreerde werkprocessen: Informatiebeheer is geen taak die achteraf wordt uitgevoerd. Het wordt een integraal onderdeel van de dagelijkse werkprocessen, van het opstellen van een brief tot het invoeren van een klantgeven.
- Verantwoordelijkheid bij de bron: Eigenaarschap van informatie wordt belegd bij de functionaris die de informatie creëert. Dit leidt tot een groter bewustzijn van het belang van correcte en tijdige registratie.
- Cultuur van openheid: Medewerkers zijn zich bewust van hun rol in het creëren van publiek goed en handelen vanuit het uitgangspunt van openbaarmaking.
- Invloed van (keten)partners: Samenwerking met (keten)partners is onlosmakelijk van belang in het informatiebeheer. Met partners moeten afspraken over informatiebeheer worden gemaakt, wederzijds wie, waarvoor verantwoordelijk is welke informatie aan wederzijdse kant vastgelegd, bewaard en vernietigd wordt.
- Toepassen van een sterke functie van conserveren en het ter beschikking stellen van informatie: Als publieke organisatie is de gemeente verplicht om eeuwig te bewaren informatie te conserveren, als een specialisatie van het DUTO proces 'bewaren van overheidsinformatie'. Met het conserveren van informatie komt ook het 'ter beschikking stellen van overheidsinformatie'. De gemeente werkt aan het stevig neerzetten van deze twee aspecten zodat de publieke waarde en openbaarheid geborgd wordt.

#### 2. Informatie- en Data-implicaties:

- Metadata-standaarden: Vanaf het moment van creatie wordt informatie voorzien van metadata, zoals de datum, de auteur, de herkomst en de classificatie. Zonder de juiste metadata is het namelijk niet mogelijk om verantwoord te bewaren en/of vernietigen.

- Uniforme taxonomieën: De gemeente hanteert een gestandaardiseerde, uniforme manier van archiveren en classificeren, zodat informatie altijd vindbaar is, ongeacht de afdeling of het systeem.
- Belang van vernietigen: De gemeente is consequent in het vernietigen van informatie die de gemeente niet meer mag hebben. Voldoen aan DUTO heeft soms niet zozeer met bewaren van informatie te maken, maar ook met het identificeren van bronnen waar informatie vernietigt moet worden, en dit dan ook daadwerkelijk doen. Door dit consequent te doen, beschermen wij de privacy van inwoners en tijdige vernietiging verkleint het risico op data incidenten. Daarnaast zijn er ook voordelen zoals: minder achterhaalde data in de systemen, lagere kosten, vergemakkelijking van conversies en migraties.

### 3. Applicatie- en Technologie-implicaties:

- Mogelijkheid op vernietiging: Applicaties van de gemeente waar te vernietigen informatie in staat, moeten wel in staat zijn om informatie daadwerkelijk te vernietigen. Nieuw aangeschafte informatievoorziening moet voldoen aan de gestelde functionaliteit voor vernietigen, of er moet een mogelijkheid zijn om met 'third party' software de vernietiging te realiseren, bijvoorbeeld door een archief beheer component in de Common ground architectuur.
- Modulaire systemen: Systemen worden gebouwd of aangeschaft met functionaliteit voor gestructureerd informatiebeheer.
- Automatisering: Waar mogelijk wordt automatisering toegepast om het vastleggen en classificeren van informatie te vergemakkelijken, bijvoorbeeld door het gebruik van slimme workflows en sjablonen.

## 7 Privacy

*De gemeente Zwolle borgt de privacy, integriteit en ethische omgang met persoonsgegevens door de vanaf de initiële ontwerpfase in processen en systemen in te bouwen (privacy by design). Dit garandeert continue en aantoonbare naleving van wet- en regelgeving (zoals de AVG) en waarborgt het publieke vertrouwen in de gemeentelijke dienstverlening.*

### Rationale:

- Wettelijke noodzaak en efficiëntie: Naleving van de AVG is verplicht. Door privacy in de ontwerpfase mee te nemen, wordt voorkomen dat dure en tijdrovende aanpassingen achteraf moeten worden doorgevoerd. Dit is een direct gevolg van de Privacy by design-eis in de AVG en sluit aan bij de NORAeis voor 'Ingebouwde beveiliging en privacy'.
- Vertrouwen en legitimiteit: Voor een overheidsorganisatie is het vertrouwen van burgers het belangrijkste bezit. Het ethisch omgaan met data - dat wil zeggen: data niet gebruiken voor doelen waar burgers niet mee instemden of die hun belangen schaden - is de basis voor dit vertrouwen. Dit gaat verder dan alleen de wettelijke minimum.
- Conformerend met referentiearchitecturen: Dit principe verankert het gebruik van de GEMMA-standaarden voor gegevensbeheer en -uitwisseling, waarbij autorisatie en doelbinding centraal staan. Het dwingt af dat de organisatie de GEMMA volgt en de NORA-principes voor privacy en beveiliging toepast.

## Implicaties:

### 1. Bedrijfskundige implicaties:

- **DPIA als poortwachter:** Het uitvoeren van een pre-DPIA is verplicht bij de start van elk project dat persoonsgegevens verwerkt. Indien de verwerking een hoog risico met zich meebrengt wordt altijd een DPIA uitgevoerd. Dit proces fungeert als de poortwachter om te beoordelen of het ontwerp voldoet aan de privacyeisen.
- **Afspraken met (keten)partners:** In de context van de 'extended enterprise' moeten er duidelijke verwerkersovereenkomsten en afspraken over doelbinding zijn met alle ketenpartners, conform de AVG.
- **Ethische toetsing:** het proces voor het ethisch toetsen moet gehandhaafd blijven, zeker bij nieuwe (datagedreven) toepassingen (bijvoorbeeld het gebruik van algoritmes).

### 2. Informatie- en Data-implicaties:

- **Dataminimalisatie:** Het uitgangspunt is het verzamelen en opslaan van zo min mogelijk persoonsgegevens. Processen moeten automatisch overbodige of niet-relevante gegevens verwijderen.
- **Pseudonimisering en anonimisering:** Waar mogelijk moeten persoonsgegevens worden gepseudonimiseerd of geanonimiseerd. De architectuur moet de technologie en processen ondersteunen om dit te kunnen doen en de herleidbaarheid strikt te beheren.
- **Transparantie en inzicht:** De architectuur moet het mogelijk maken dat burgers inzicht krijgen in welke gegevens de gemeente over hen verwerkt, en waarvoor (recht op inzage, art. 15 AVG).
- **Doelbinding:** Persoonsgegevens mogen enkel worden verzameld door welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder worden verwerkt op een wijze die onverenigbaar is met die doeleinden.

### 3. Applicatie- en Technologie-implicaties:

- **Strikte scheiding van functionaliteiten:** Applicaties moeten zodanig ontworpen zijn dat de verwerking van persoonsgegevens gescheiden is van de algemene functionaliteit (scheiding van rollen en rechten).
- **Standaardisatie van beveiligingscomponenten:** Er wordt gebruikgemaakt van gestandaardiseerde, getoetste technische componenten voor authenticatie, autorisatie en encryptie (versleuteling) die voldoen aan de BIO (Baseline Informatiebeveiliging Overheid) - die voortbouwt op de ISO 27000-serie - om de technische basis voor Privacy by design te leggen.
- **Toegangsbeheer op maat:** De technologie moet zorgen voor fijnmazige toegangscontrole die is afgestemd op de gevoeligheid van de gegevens en de specifieke rol van de gebruiker (zero-trust-gedachte).