Inhoud

1 Informatievoorziening architectuurprincipes 2
1.1 Component gebaseerd – volgens lagenmodel 2
1.2 Open 3
1.3 Vertrouwd 4
1.4 Eenmalige vastlegging 5
1.5 Regie op gegevens 7
1.6 Standaard 7

1 Informatievoorziening architectuurprincipes

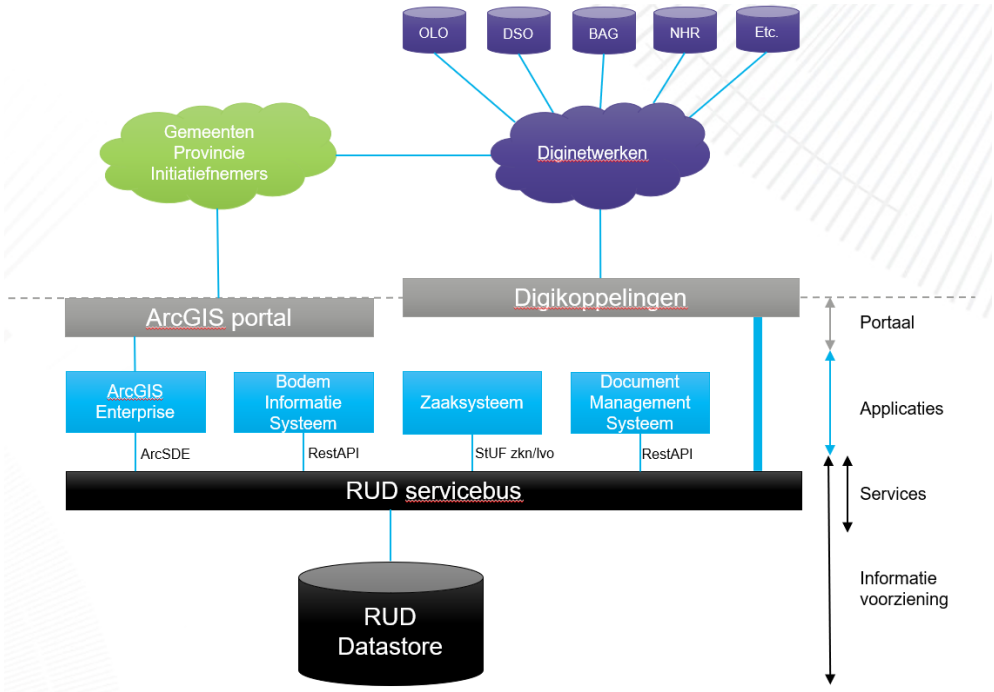
Deze notitie beschrijft de door de RUD Utrecht gehanteerde informatiearchitectuur-principes; een aantal fundamentele keuzes die richting geven aan hoe er binnen het nieuwe landschap met gegevens en applicaties moet worden omgegaan. Deze principes zijn sterk verbonden met de realisatieprincipes voor de Common Ground.

De principes zijn bedoeld om 'just enough' richting te geven aan nieuwe ontwikkelingen. Bij het ontwerpen van nieuwe of aangepaste voorzieningen moet worden aangegeven hoe invulling wordt gegeven aan de principes, en welke overwegingen daarbij worden gemaakt. Daarbij geldt het pas-toe-of-leg-uit principe. Afwijkingen alleen zijn toegestaan als ze met goede argumenten worden onderbouwd en vastgelegd om daar in een later stadium op terug te kunnen komen. Zo wordt voorkomen dat belangrijke zaken over het hoofd worden gezien, en wordt geborgd dat activiteiten in lijn zijn met uitgangspunten van het RUD Utrecht informatiebeleid.

GEMMA als referentiearchitectuur kent al principes die de RUD Utrecht helpt om met name het interne Informatieseringsbeleid goed in te richten. De informatiearchitectuur-principes zijn in lijn met de GEMMA-principes maar zijn concreter van aard en gericht op het gezamenlijk ontwikkelen van de beoogde nieuwe informatiehuishouding.

1.1 Component gebaseerd – volgens lagenmodel

De RUD Utrecht werkt met componenten (applicatie en services) die afgebakende functionaliteit kennen en via gestandaardiseerde interfaces communiceren in plaats van met grote geïntegreerde (silo)systemen. We gebruiken hierbij een lagenmodel waarin we onderscheid maken tussen minimaal 'interactie', 'applicatieprocessen', 'integratie en services' en 'gegevens'. Een hierop gebaseerd informatielandschap stelt de RUD Utrecht in staat om wendbaar en innovatief te opereren omdat wijziging of vervanging per component mogelijk wordt.



Figuur 1 : Voorbeeld lagenmodel

1) De diensten die componenten leveren worden ontworpen en gebruikt volgens gangbare service-oriëntatie principes.
   a) Autonomie - Componenten zijn zelfstandig inzetbaar, schaalbaar en vervangbaar.
   b) Losse koppeling - Componenten zijn onderling onafhankelijk en zelfstandig door te ontwikkelen en gebruiken. Wanneer één component niet beschikbaar is, blijven andere componenten functioneren.
   c) Herbruikbaar - Componenten zijn vaker in te zetten door ze in verschillende omgevingen te gebruiken of door een component vaker te instantiëren binnen één omgeving.
   d) Samenstelbaar - Componenten kunnen worden gecombineerd tot nieuwe componenten.
   e) Abstractie - Afnemers hoeven alleen de functionaliteit, niet de interne werking, van een component te kennen.
   f) Servicecontract - Een component kent duidelijke voorwaarden en leveringsafspraken over de kwaliteit en het volume van mogelijk gebruik door afnemers.
   g) Vindbaar - Services zijn voorzien van metadata en zijn goed vindbaar.
   h) Toestandloos - Componenten hoeven zelf geen statusinformatie bij te houden zodat impact op opslag minimaal is en performance maximaal is.
2) Componenten leveren conform opgestelde specificaties
   a) Functies (doet wat beschreven is dat hij moet doen).
   b) Interfaces (biedt en gebruikt beschreven interfaces).
   c) Standaarden (gebruikt verplicht gestelde standaarden)
   d) Niet-functionele capaciteiten (bijvoorbeeld voor beveiliging en logging).
3) Componenten conformeren zich aan het Common Ground-lagenmodel, wat impliceert:
   a) Componenten beperken zich tot functionaliteit binnen de laag waartoe ze behoren (bijvoorbeeld een frontend-applicatie beperkt zich tot presentatie en kent geen vastlegging van brongegevens). Als er goede redenen voor zijn, mag een component conform het pas-toe-of-leg-uit principe ook functionaliteit uit de onderliggende laag realiseren (bijvoorbeeld een front-end-applicatie die (ook) procesfunctionaliteit bevat omdat er daarvoor geen bruikbare component beschikbaar is).
   b) Componenten voor interactie- en procesfunctionaliteit vragen gegevens op bij de bron via gestandaardiseerde interfaces (bijvoorbeeld een app vraagt brongegevens op via aanroep van een standaard API).
   c) Componenten bewerken geen brongegevens anders dan bij de bron (bijvoorbeeld een app corrigeert een opgevraagd brongegeven niet in een lokale schaduwregistratie maar ondersteunt het aanpassen van het betreffende gegeven in de bronregistratie).
   d) Mobiele componenten zoals apps richten zich op specifieke dienstverlening (bijvoorbeeld een app waarmee toezichthouders gericht worden geïnformeerd t.a.v.).
4) Componenten voldoen bij gebruik aan de voor gemeenten van toepassing zijnde standaarden voor informatiebeveiliging, authenticatie, autorisatie en logging (de Baseline Informatiebeveiliging Gemeenten BIG). Naast componentgebonden functionaliteit kan dit ook (deels) worden gerealiseerd door voorzieningen in de ICT infrastructuur waar componenten actief zijn.

1.2 Open

De overheid stelt hoge eisen aan de transparantie van overheidsorganisaties. De RUD Utrecht wil transparant zijn in hoe we informatie en software gebruiken. Door als RUD Utrecht open te zijn waar dit kan, wordt de informatiepositie van gemeenten, provincie en initiatiefnemers versterkt, wordt publiek/private samenwerking gefaciliteerd en neemt het vertrouwen in de overheid toe.

1) Indien beschikbaar gebruiken we open standaarden die publiekelijk beschikbaar zijn en waarvan de specificaties vrij van licentierechten mogen worden toegepast, gebruikt en gehanteerd.
2) Gegevens worden conform de geldende bewaar- en vernietigingstermijnen uit de vigerende wet- en regelgeving behandeld. Gegevens worden waar dat vereist is gearchiveerd, vernietigd en duurzaam opgeslagen en beschikbaar gesteld.
3) Digitale voorzieningen voor het interactief opvragen van gegevens voldoen aan wettelijke eisen rondom digitale toegankelijkheid zodat voorzieningen bruikbaar zijn voor alle gemeenten, Provincie en initiatiefnemers.
4) Alle gegevensverzamelingen die maatschappelijk of economisch waardevol zijn en waarvoor geen beperkingen vanuit wetgeving of hun classificatie gelden worden waar mogelijk als open data beschikbaar gesteld.
5) Bij het ontwerpen en implementeren van bronregistraties wordt rekening gehouden met beschikbaarstelling daarvan in de vorm van open data (bijvoorbeeld door gegevens geanonimiseerd te kunnen verstrekken).

1.3 Vertrouwd

In de steeds meer informatie gestuurde werkprocessen moeten provincie, gemeenten en initiatiefnemers kunnen blijven vertrouwen op de integriteit van de RUD Utrecht. We garanderen daarvoor dat we ons houden aan wettelijke richtlijnen, nemen maatregelen om risico's te minimaliseren, en verantwoorden naar betrokkenen wat we doen. We zorgen voor een goede beveiliging van gegevens en garanderen privacy. Om invulling te kunnen geven aan zowel verwachtingen van de burger als de wettelijke vereisten realiseren we een samenhangend geheel van technische, organisatorische, fysieke en procedurele maatregelen.

1) Informatiebeveiliging en privacy worden integraal meegenomen bij het ontwerp en de inrichting van applicaties en infrastructuur ('privacy en security by design'; we besteden er vanaf de start aandacht aan en niet pas aan het einde).
2) Het doel waarvoor gegevens gebruikt mogen worden is vastgelegd in wet- en regelgeving. We verwerken gegevens conform wet en regelgeving (bijvoorbeeld door controles op doelbinding en voldoen aan de beginselen van subsidiariteit en proportionaliteit voordat gegevens worden verstrekt).
3) Bij nieuwe voorzieningen zijn standaardconfiguratie-instellingen de meest veilige instellingen ('security en privacy by default'; functionaliteit die niet nodig is wordt uitgeschakeld).
4) Als verwerker van gegevens nemen we maatregelen om risico's te beperken zoals het minimaliseren, scheiden, abstraheren of verbergen van gegevens (bijvoorbeeld niet meer gegevens verstrekken dan nodig is voor het doel).
5) Als verwerker van informatie laten we zien zorgvuldig om te gaan met gegevens door maatregelen zoals het informeren van betrokkenen en het transparant zijn over plaatsgevonden gegevensgebruik en verantwoording daarvan (bijvoorbeeld door het actief bieden van inzicht in de verwerking van hun gegevens).
6) Private of openbare netwerken die voor gegevensuitwisseling gebruikt worden, worden passend bij het vereiste betrouwbaarheidsniveau van diensten, afdoende beveiligd, gemonitord en geanalyseerd (bijvoorbeeld door in situaties waarin partijen garanties nodig hebben over de identiteit van de andere partij gebruik te maken van geschikte certificaten).
7) Als gegevenshouder bewaken we de toegang tot vertrouwelijke gegevens, en maken afspraken met afnemers van gegevens over gebruik daarvan. Bij afwijking van de afspraken nemen we

passende maatregelen (bijvoorbeeld door toegang tot gegevens te blokkeren of melding te maken van misbruik van gegevens bij de Autoriteit Persoonsgegevens).

8) Afnemers van gegevens zijn zelf verantwoordelijk voor behoorlijk gegevensgebruik. Afnemen van gegevens impliceert dus een verantwoordelijkheid bij de afnemer die zich bijvoorbeeld via een toestemmingsverklaring hiermee akkoord verklaart (bijvoorbeeld wanneer een derde partij gegevens van de RUD Utrecht ontvangt).
9) Bij uitwisseling van gegevens vindt authenticatie plaats op het niveau van de identiteit van de afnemende organisatie ('gedelegeerde autorisatie'). De afnemende organisatie is verantwoordelijk om daar waar nodig gebruikers te authentiseren en te autoriseren (bijvoorbeeld door op basis van uit te voeren werkzaamheden te bepalen tot welke gegevens een gebruiker toegang krijgt).
10) Een afnemende organisatie is verplicht een verwerkingenregister conform de AVG met gestandaardiseerde doelbindingsclaims te gebruiken (conform een door gemeenten gestandaardiseerd informatiemodel).
11) Ieder verzoek om gegevens wordt voorzien van een 'doelbindingsclaim' die wordt vastgelegd om mede aan de hand hiervan te kunnen vaststellen of een plaatsgevonden verwerking rechtmatig was (bijvoorbeeld bij het gebruik van persoonsgegevens).
12) Iedere gegevensuitwisseling wordt gelogd met als doel om een sluitende audit trail van informatietransacties te vormen (bijvoorbeeld door zowel aan de kant van de aanvrager als de leverancier van gegevens in samenhang op te vragen logginggegevens vast te leggen).
13) De integriteit van logbestanden wordt bewaakt (bijvoorbeeld door het gebruik van checksums waarmee is te constateren of bestanden gewijzigd zijn).
14) Logbestanden zijn duurzaam toegankelijk, geschikt voor audits, en voor het kunnen inzien van persoonsgebonden informatie door burgers. We sturen actief op het zorgvuldig loggen in een standaard formaat om logbestanden maximaal bruikbaar te maken.
15) In algemene zin geldt dat informatiebeveiligingsmaatregelen voldoen aan de voor gemeenten van toepassing zijnde strategische en tactische baseline informatiebeveiliging, de BIV-classificatie van de betrokken onderdelen, en een risicoanalyse vanuit procesperspectief.
16) Gegevens worden conform de geldende bewaar- en vernietigingstermijnen uit de vigerende wet- en regelgeving behandeld. Gegevens worden waar dat wordt vereist gearchiveerd, vernietigd en/of duurzaam opgeslagen en beschikbaar gesteld.

1.4 Eenmalige vastlegging

De RUD Utrecht wint gegevens eenmalig in, leggen ze eenmalig vast en gebruiken ze vervolgens, overeenkomstig het doel waarvoor ze ingewonnen zijn, meervoudig. Net zoals bij de landelijke basisregistraties is gebeurd, standaardiseren we ook andere bronbestanden en ontwikkelen hiermee RUD kernregistraties. Eenmalig opgeslagen brongegevens worden alleen bewerkt bij de bron en komen beschikbaar voor processen die ze nodig hebben. Die slaan geen kopieën van die gegevens meer op maar vragen ze via gestandaardiseerde interfaces op bij de bron.

1) Ten aanzien van bronregistraties geldt:
   a) Bij bronregistraties standaardiseert de bronhouder in overleg met stakeholders de semantiek, syntax en samenhang van gegevens.
   b) Voor de RUD Utrecht vindt deze standaardisatie plaats onder regie van gemeenten en Provincie Utrecht (bijvoorbeeld bij het opstellen van nieuwe informatiemodellen).
   c) Kernregistraties (bronhouder RUD Utrecht) worden beschreven m.b.v. een standaard informatiemodel.

d) Gegevens kennen één bron (dat kan een bronregistratie per gemeente zijn).
e) Iedere gegevensbron heeft een eigenaar die verantwoordelijk is voor beschikbaarheid, integriteit, vertrouwelijkheid, volledigheid en kwaliteit.
f) Bij ieder gegeven is, voorzover mogelijk aangegeven welke kwaliteit het heeft om de bruikbaarheid te kunnen vaststellen.
g) Bronregistraties en daarvan afgeleide diensten ondersteunen formele en materiële historie (bijvoorbeeld om te kunnen constateren vanaf welk moment een nieuw adres administratief was vastgelegd).
h) Bij gegevensuitwisseling maken bronhouder en gebruiker afspraken door middel van een gegevensleverings- en verwerkersovereenkomst (bijvoorbeeld over doel en gebruikstermijn).
i) Vermeende onjuistheden in gegevens worden door afnemers teruggemeld aan de desbetreffende bronhouder.
j) Gegevensbronnen maken hergebruik van basisregistraties.

2) Ten aanzien van uitwisseling en beschikbaarstelling geldt:
a) Brongegevens worden niet binnen procesapplicaties opgeslagen (bijvoorbeeld door mutaties in brongegevens niet langer te ontvangen en kopie-gegevens binnen procesregistraties bij te werken).
b) Er vindt geen gegevensdistributie plaats; een proces kan worden genotificeerd over een gebeurtenis waarna de ontvangende applicatie de benodigde gegevens kan opvragen (“informatie-arm notificeren”).
c) Brongegevens worden, bij voorkeur realtime, opgehaald bij de bron (bijvoorbeeld door via een service gegevens op te halen op het moment dat ze nodig zijn).
d) Gegevensuitwisselingen zijn uniek identificeerbaar, worden gelogd en voorzien van relevante contextinformatie en metadata; dit alles binnen wettelijke kaders en mogelijke afwijking in bijzondere gevallen (bijvoorbeeld bij criminaliteitsbestrijding, terrorisme, ondermijning, fraudebestrijding).
e) Voor uitwisseling van gegevens wordt gebruik gemaakt van services met gestandaardiseerde API’s (bijvoorbeeld door REST-services berichten in JSON formaat uit te wisselen).
f) De manier waarop gegevens worden geleverd past bij de gevoeligheid van betrokken gegevens (bijvoorbeeld vertrouwelijke gegevens alleen via veilige kanalen en netwerken, belangrijke transactiegegevens met gegarandeerde aflevering).
g) Gegevens en bedrijfsregels worden beschikbaar gesteld via services die beschikken over gestandaardiseerde interfaces die:
    i) beschreven zijn met standaard beschrijvingstalen (protocol).
    ii) vindbaar zijn in een centrale catalogus.
    iii) aangeboden worden via integratievoorzieningen (bijvoorbeeld via een API-gateway).
    iv) alleen bruikbaar zijn na afdoende authenticatie en autorisatie (bijvoorbeeld via het gebruik van certificaten).
h) Gegevensdiensten zijn atomair, consistent, isoleerbaar en duurzaam (bijvoorbeeld bij transacties waarbij meerdere partijen betrokken zijn).
i) Informatie- en gegevensdiensten verstrekken gegevens proportioneel en subsidiair. Gegevensleveringen worden ‘smal’ gehouden en bevatten niet meer gegevens dan wat noodzakelijk is voor het verwerkingsdoel (bijvoorbeeld door toegestane persoonsgegevens bij een verstrekking te minimaliseren en die op een voldoende veilige manier te verstrekken).
j) Gegevens moeten zodanig beschikbaar zijn dat interactie tijd-, plaats- en apparaatonafhankelijk kan plaatsvinden (bijvoorbeeld door 24x7 brongegevens beschikbaar te stellen die via mobiele apps zijn op te vragen).

k) Voor interactie-applicaties geldt dat als ophalen van brongegevens niet mogelijk is, en lokale opslag om functionele redenen vereist is, er bij gebruik van vertrouwelijke gegevens hoge beveiligingsmaatregelen nodig zijn (bijvoorbeeld bij apps die gebruikt moeten worden in omstandigheden waarin geen netwerk beschikbaar is).

1.5 Regie op gegevens

Partijen die daartoe gerechtigd zijn, moeten regie kunnen voeren op welke gegevens aan wie, op welk moment en voor welk doel, worden verstrekt. Persoonlijk datamanagement draagt bij aan transparantie, inzage en correctie, digitale zelfbeschikking, privacy, dataminimalisatie, de kwaliteitsverbetering van gegevens en zelfredzaamheid van mensen. We geven daarom inzicht in wie welke gegevens bijhoudt en welke gegevens uitgewisseld worden.

1) Ten aanzien van burgers en bedrijven als partijen met zeggenschap over hun gegevens geldt:
   a) We stellen burgers in staat om hun AVG-conforme rechten op informatie, kopie, vergetelheid en beperking uit te oefenen waar dit juridisch mogelijk is, bij:
      i) hun eigen gegevens (incl. inhoudelijke dossiers en gegevens in sectorale registraties);
      ii) gegevens die zijn gebruikt om tot een besluit te komen en de regels die daarbij zijn gehanteerd (traceerbaarheid);
      iii) gegevens die zijn ingezien en gebruikt (transparantiebeginsel): burgers krijgen direct online inzicht in de actuele verwerking van hun gegevens en de daarvoor gehanteerde doelbindingsclaims.
   b) Burgers kunnen toestemming geven voor het gebruik van hun eigen gegevens bij taken waarvoor geen expliciete wettelijke grondslag bestaat (bijvoorbeeld door na een helder toegelicht verzoek met een digitale handtekening akkoord te geven voor een welomschreven gebruik van een set persoonsgegevens).
   c) Burgers en bedrijven worden proactief geïnformeerd over zaken waarvan zij hebben aangegeven dat zij daarover geïnformeerd willen worden (bijvoorbeeld door hen via notificaties op de hoogte te stellen van relevante gegevens-gerelateerde activiteiten).
2) Ten aanzien van de RUD Utrecht als gegevensverwerker geldt:
   a) De RUD Utrecht beslist binnen wettelijke kaders voor wie, welke gegevens beschikbaar worden gesteld (bijvoorbeeld door binnen applicaties zelf in te stellen welke gegevens voor derden beschikbaar komen).
   b) De RUD Utrecht bepaald hoe zij gegevens beschikbaar stellen voor gebruik door applicaties (bijvoorbeeld door te kiezen voor standaard API's die via een gemeenschappelijke integratievoorziening door derden benaderbaar zijn).

1.6 Standaard

De RUD Utrecht werkt samen Provincie Utrecht, gemeenten en steeds meer andere partijen. Afspraken en standaarden zijn nodig om effectief, efficiënt en veilig samen te werken en informatie uit te wisselen. Ze zijn ook nodig om voldoende onafhankelijk te blijven en de juiste samenwerkingspartners te kunnen kiezen. Standaardiseren is van belang binnen alle (lagen van) functionaliteit.

1) We volgen zoveel mogelijk standaarden, ook als ze niet verplicht zijn. (bijvoorbeeld door gebruik van wettelijk verplichte toegankelijkheidsstandaarden maar ook de door het Forum Standaardisatie aanbevolen standaard voor het uitwisselen van datastructuren).

2) We gebruiken waar mogelijk open standaarden conform de richtlijnen van het Forum Standaardisatie.
3) We ontwikkelen als RUD Utrecht in afstemming met leveranciers nieuwe standaarden waar deze nodig maar nog niet beschikbaar zijn (bijvoorbeeld in de vorm van informatiemodellen en API-specificaties).
4) Landelijke catalogi, voorzieningen en bouwstenen worden gebruikt waar het verplicht is en zoveel mogelijk gebruikt waar het niet verplicht maar wel mogelijk is.
5) Gegevensmodellering, ontsluiting en integratie van gegevens zijn gestandaardiseerd.
6) Logging en auditing zijn gestandaardiseerd (bijvoorbeeld informatie over doelbinding en verwerking conform gemeentelijk informatiemodel).
7) Standaarden moeten in de praktijk eenvoudig bruikbaar zijn.
8) Naast generiek toepasbare standaarden kennen we ook standaarden die taak- of functie specifiek zijn (bijvoorbeeld voor gegevensuitwisseling binnen een sector).
9) Voor gebruik van API's hanteren we de landelijke API- en URI-standaarden.
10) API's worden in een vastgesteld formaat beschreven.
11) Bij beschrijving van API's worden ook authenticatiemogelijkheden en testfaciliteiten beschreven (bijvoorbeeld door aan te geven welke authenticatiemechanismen worden ondersteund).