Bijlage 1 Ontwerp & Architectuur inclusief programma van eisen
Levering Datawarehouse Automation tool gemeente Eindhoven
Kenmerk: EHV-2022-JA-002

1. Functionele beschrijving

Gemeente Eindhoven wil data uit verschillende bronsystemen structureel opslaan in Data Warehouses volgens Data Vault methodologie, om vanuit hier, aan diverse informatiebehoeften te voldoen.

Wat

Datawarehouse Automation (DWA) oplossing (ICT-prestatie) van leverancier die het ontwerpen, ontwikkelen, beheren en inzichtelijk maken/documenteren van data automatiseert, waarbij de oplossing de mogelijkheid biedt met drag and drop een business georiënteerd ontwerp van het Data Vault te creëren, op basis waarvan alle data lagen zoals load, persistent Data Vault-stage en Data Vault automatisch gegenereerd worden. Vanuit de Data Vault laag biedt de applicatie de mogelijkheid, door middel van drag and drop functionaliteit, om Data Marts in onder andere Kimball formaat of Analyse tabellen te genereren ten behoeve van gevisualiseerde rapporten, analyses en AI.

Wie

'Data engineers, beheerders en testers van de gemeente Eindhoven (vast en inhuur) moeten gebruik kunnen maken van de Datawarehouse Automation (DWA) oplossing. Dit is geen tool voor eindgebruikers binnen de Gemeente Eindhoven.

Inschatting aantallen: Gemeente Eindhoven kent 5 domeinen: SD, BV, RD, Dienstverlening en Overig met 2 data-engineers per domein, dus circa 10 data-engineers uiteindelijk. Gemeente start met BV en SD dus 4 data-engineers.

Waar:

Vooralsnog op virtuele servers in het Data Center van Gemeente Eindhoven, later te migreren naar Cloud platform.

Data afkomstig van diverse bronsystemen, zowel on premise als SAAS. Target Database vooralsnog on premise, later te migreren naar Cloud platform.

Soort data

Openbare, vertrouwelijke data, intern gebruik, AVG Privacy gevoelige data, archiefwaardige data en financiële data

.

2. Proces

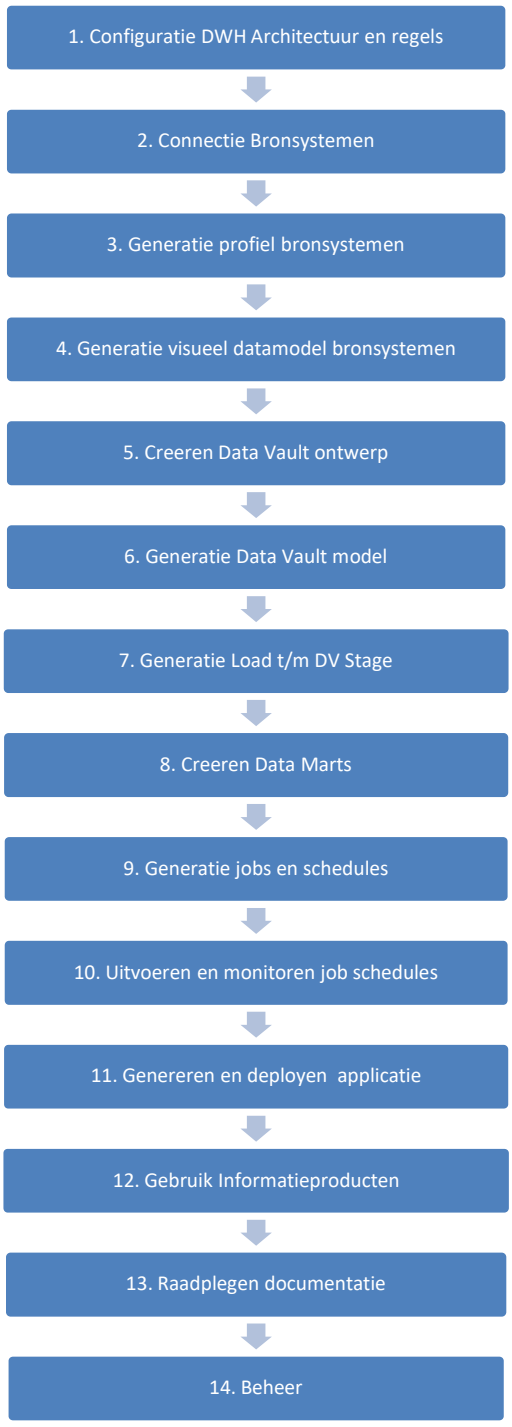
In dit hoofdstuk wordt het te ondersteunen proces toegelicht. Daarna worden de nadere functionele eisen waaraan dit proces moet voldoen benoemd.

Proces Data Vault ontwerpen en ontwikkelen

Doel proces

Geautomatiseerd ontwerpen en ontwikkelen van Data Vault en Data Mart inclusief alle bijbehorende lagen.

De ICT-oplossing faciliteert de volgende processtappen:



Hieronder worden de processtappen verder uitgeschreven met, waar van toepassing, per processtap (of groep van stappen) de bijbehorende eisen.

1. Configureren van de gewenste data architectuur lagen en bijbehorende conversie regels die nodig zijn voor het automatisch genereren.
   Eis 1.1 Uw oplossing biedt de mogelijkheid om de data architectuur lagen en de manier waarop deze geautomatiseerd worden opgebouwd volledig te configureren, waaronder in ieder geval de volgende zaken;
   bepalen welke lagen worden opgenomen (load, persistent staging area etc), naamgevingsconventies, metadata-standaarden, naamgeving van de lagen, opschoningsregels, creëren van standaard metadata-velden, regels voor opbouwen van historie, regels voor het gebruik van hashkeys.

2. Connecteren met diverse bronsystemen.
   Eis 2.1 Uw oplossing biedt minimaal de mogelijkheid om CSV en Excel bestanden in te lezen.

3. Profileren van brontabellen.
   Eis 3.1 Uw oplossing biedt de mogelijkheid automatisch metadata te extraheren uit de bronapplicaties, met minimaal de volgende kenmerken: veldnamen, data type en veldlengte. EIS

4. Automatisch creëren van visueel model van de bronapplicatie op basis metadata bronsysteem.

5. Maken van een (visueel) Core-Business-Concept (CBC) driven (‘business-driven’) Data Vault ontwerp inclusief definities.
   Eis 5.1 Uw business gedreven DataVault Ontwerp / Automatisering oplossing biedt de mogelijkheid om data modellen te creëren die gebaseerd zijn op business ontwerpen en niet op de bronstructuur (de oplossing wordt niet uitgevoerd door standaardscripts die op basis van het bronsysteem tabellen transformeren naar HUB's, Links en Satellieten).
   Eis 5.2 Uw oplossing biedt een visuele 'drag en drop' gebruikersinterface voor het ontwerpen van een Data Vault, het toewijzen van de bronvelden aan de ontworpen Data Vault velden en het leggen van relaties tussen de Data Vault entiteiten.

6. Geautomatiseerd creëren code voor een Data Vault Model inclusief alle benodigde metadata velden op basis van het CBC gebaseerd ontwerp.
   Eis 6.1 Op basis van het business ontwerp van het DV model moeten het feitelijke DV model en bijbehorende code automatisch worden afgeleid en gecreëerd inclusief alle benodigde metadata velden. Handmatig coderen is niet nodig.

7. Geautomatiseerd creëren van de in stap 1 gedefinieerde en geconfigureerde code voor de lagen vanaf de brontabellen tot het Data Vault.
   Eis 7.1 Uw oplossing biedt de mogelijkheid om op basis van het Data Vault ontwerp automatisch code te genereren voor zowel alle load- en transformatiescripts als het creëren van alle tabellen voor alle lagen vanaf de brontabellen tot en met het Data Vault.

8. Creëren van Data Marts
9. Geautomatiseerd creëren van jobs en schedules voor het tijdig en in de juiste volgorde laten lopen van alle code.
10. Uitvoeren van schedules en monitoren van jobs.

Eis 8-10.1 Uw oplossing biedt een visuele drag en drop gebruikersinterface voor het ontwerpen en mappen van het Data Marts in Kimball format of andere modelvormen.

Eis 8-10.2 Uw oplossing biedt de mogelijkheid om voor ontworpen Data Marts of Analyse tabellen automatisch de code te genereren voor zowel het creëren van de tabellen en views als voor de scripts die de data extraheren, transformeren en laden. Uitzonderingen zijn stukjes code voor specifiek business rules of transformaties.

11. Creëren van volledige data integratie applicaties inclusief scheduling en promotie naar Test, Acceptatie en Productie omgeving.

12. Gebruik informatieproducten (Buiten applicatie)

13. Raadplegen documentatie
14. Beheer

Eis 13-14.1 Uw oplossing biedt visuele weergaven van alle data modellen die in metadata beschikbaar zijn, van bron tot en met Data Mart.

Eis 13-14.2 Uw oplossing biedt zowel een visuele als een tekstuele weergave van de volledige data lineage. Elk willekeurig dataobject van brontabel tot en met de laatste binnen de applicatie geproduceerde informatieproducten zijn hier in opgenomen. Vanuit elk willekeurig dataobject in de data integratiestraat kan de lineage bekeken worden tot het laatste object, zowel upstream als downstream.

Eis 13-14.3 Uw oplossing biedt de mogelijkheid om velddefinities vast te leggen in het Data Vault design. De definities worden overgenomen naar alle dataproducten die hier van de Data Vault laag worden afgeleid. Ook de definities voor de afgeleide velden zijn in de documentatie automatisch beschikbaar.

Eis 13-14.4 Uw oplossing biedt de mogelijkheid op basis van de selectie van een subset van de tabellen in de Data Integratiestraat een Data Glossary of Data Dictionary te genereren, gebaseerd op de beschikbare metadata zoals datatype, lengte en de vastgelegde definities.

Eis 13-14.5 Uw oplossing is zelf-documenterend voor alle gecreëerde metadata, zowel in visuele vorm met data modellen en data lineage, als in tekstuele vorm, inclusief alle metadata en definities op veldniveau.

Eis 13-14.6 De documentatie die uw applicatie genereert is zowel in de applicatie te bekijken als te exporteren in HTML en pdf formaat.

Algemene functionele eisen

Eis Alg 01 Uw oplossing kan code genereren voor meerdere database typen, maar tenminste voor MS Sql, Oracle, Snowflake en PostgreSQL.

Eis Alg 02 Alle code moet open toegankelijk zijn voor controle, bewerking, aanpassing en onderhoud.

3. Niet-Functionele Eisen

In dit hoofdstuk worden de niet-functionele eisen benoemd waaraan uw ict-oplossing moet voldoen.

1. Uw oplossing kan draaien binnen de Azure cloud omgeving. - EIS

3.1 Informatiebeheer

1. De ICT Prestatie biedt de mogelijkheid tot geavanceerd zoeken (op basis van zelf te kiezen filters). – EIS
2. De ICT Prestatie biedt de mogelijkheid om op procesniveau in te richten wat er moet gebeuren bij het uitvoeren van een vernietigingsactie. Gegevens moeten bewaard, verwijderd of geanonimiseerd kunnen worden. – EIS
3. Informatieobjecten, gegevens en bijbehorende metadata (op verschillende aggregatieniveaus: dossier/zaak en onderliggende documenten, bestanden, elementen in een database, koppelingen met klantprofielen of persoonsgegevens) moeten onherstelbaar kunnen worden vernietigd op basis van de als zoekcriteria opgegeven metadata. Er is geen limiet aan het aantal items dat vernietigd kan worden. – EIS
4. Wanneer voor zoeken en vinden gebruik wordt gemaakt van indexering, dient de index na vernietiging te worden geactualiseerd zodat vernietigde informatie niet meer gevonden kan worden. – EIS

3.2 Functioneel beheer

1. Functioneel beheerders van de Opdrachtgever hebben de mogelijkheid om functionele parameters, stuurgegevens en meldingen aan te passen/onderhouden. – EIS
2. Implementeren van de ontwikkeling, test en acceptatie (OTA) omgeving naar productie wordt zonder overtypen uitgevoerd. – EIS
3. Bij nieuwe releases van de Programmatuur blijven bestaande gegevens in de applicatie toegankelijk zonder verandering van inhoud en structuur en verlies van functionaliteit. Oorspronkelijke metadata blijven behouden. – EIS

3.3 Technisch beheer

3.3.1 Database (standaardisatie)

1. De ICT Prestatie maakt uitsluitend gebruik van database versies die door de database-leverancier (Derden Programmatuur - GIBIT) worden ondersteund én die niet onder de extended support regelingen vallen. – EIS
2. De ICT Prestatie maakt uitsluitend gebruik van Oracle Enterprise, MS SQL Server Enterprise of PostgreSQL database versies. – EIS
3. De door de Leverancier toegepaste database kan op een shared database server draaien, los van de applicatieserver. – EIS
4. In de door de Leverancier aangeboden ICT Prestatie wordt er vanuit de client- en/of applicatieserver verbinding gemaakt naar de databaseserver, door middel van een alias (i.p.v. een IP adres of database servernaam). – EIS
5. U past uitsluitend databases toe die gemonitoord kunnen worden m.b.v. de monitortool OEM (Oracle Enterprise Manager). – EIS
6. In de door de Leverancier aangeboden ICT Prestatie worden de gebruikers van de Programmatuur aangemaakt vanuit de Programmatuur en niet vanuit de database of beiden. -EIS

3.3.2 Database (Security)

1. In de door de Leverancier aangeboden ICT Prestatie worden er geen DBA rechten of soortgelijke rechten gebruikt voor gebruikers of schema-eigenaren in de database na installatie. – EIS

2. Er komen geen embedded databases passwords (hardgecodeerde wachtwoorden in de broncode) in de Programmatuur voor. – EIS
3. Er komen geen unencrypted database passwords in de configfiles van de Programmatuur voor. – EIS
4. In de door u aangeboden ICT Prestatie wordt bij het aanmaken van een nieuwe database-user via de Programmatuur afgedwongen dat het password voldoet aan de password-richtlijnen van Opdrachtgever. – EIS
5. De ICT Prestatie functioneert op basis 'Principle of last privilege' voor databaserechten. – EIS
6. De database van de ICT Prestatie functioneert op basis van Role based Acces control (rechten aan gebruikers toekennen via rollen en niet rechtstreeks rechten toekennen aan de gebruikers). -EIS

3.3.3 Server applicatie

1. Indien de aangeboden ICT prestatie gebruik maakt van een onpremise webserver zijn de volgende technische eisen van toepassing:
   Alle webservers
   - Moet voldoen aan de nieuwste CIS benchmark welke van toepassing is op de aangeboden oplossing.
   Alle webservers behalve IIS
   - Leverancier staat in voor en is verantwoordelijk voor de updates en/of upgrades van de aangeboden oplossing - EIS
2. Alle default account en wachtwoorden worden bij of voor oplevering door de Leverancier gewijzigd. Dit geldt ook voor de standaard applicatie accounts van de Programmatuur zoals bv ‘system’ en ‘manager’ in een oracle database. Na oplevering zijn deze periodiek door Opdrachtgever aanpasbaar. De Leverancier levert hiervoor een handleiding aan en verschaft alle account gegevens aan Opdrachtgever. – EIS
3. De ICT Prestatie kan overweg met UNC paden (DFS namespacing). – EIS

3.3.4 Technisch algemeen

1. Vanuit de ICT Prestatie worden er geen bedrijf kritische of privacy gevoelige data op het (virtuele of fysieke) device(s) van de Programmatuur opgeslagen. Deze data wordt uitsluitend in een gecontroleerde centrale omgeving opgeslagen. – EIS
2. De ICT Prestatie wordt conform het OTAP principe ingericht. In de OTA omgeving worden enkel fictieve data gebruikt. De ICT prestatie moet hiervoor geschikt zijn. - EIS
3. De installatie van de OTA omgeving wordt uitgevoerd op een door de Opdrachtgever aangeboden afzonderlijke Active Directory met gekoppelde Azure AD-Tentant. De ICT prestatie moet hiervoor geschikt zijn. – EIS
4. De ICT Prestatie voorziet in validatiecontroles in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken. Er zijn door Leverancier beheersmaatregelen geïmplementeerd voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen. – EIS
5. Applicatie server kan overweg met vmWare vmotion. Het is niet mogelijk om licenties te koppelen aan hardware id. – EIS
6. De ICT Prestatie ondersteunt installatie op een virtueel server Operating System.
7. De ICT Prestatie maakt gebruik van een centrale geregelde licentie server i.p.v. losse individuele licenties rechtstreeks geinstalleerd op het endpoint device. – EIS
8. De ICT Prestatie bevat mechanismen voor normalisatie en validatie van invoer en voor schoning van uitvoer. – EIS
9. De ICT Prestatie gaat om met diakrieten. – EIS
10. De ICT Prestatie ondersteunt zowel IPv4 als IPv6. – EIS

11. Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als dit noodzakelijk is. – EIS
12. Alle protocollen die worden gebruikt en staan in de verplichte standaarden van Forum Standaardisatie voldoen aan de vereiste versie of hoger. https://www.forumstandaardisatie.nl/open-standaarden/verplicht

3.3.5 Certificaten

1. Bij interne certificaten gebruikt Leverancier geen Self Signed of WildCard certificaten. De aangeboden oplossing kan overweg met de Opdrachtgever CA aangeboden certificaten. – EIS
2. Bij gebruik van een subdomein of domein dat door de Opdrachtgever wordt beheerd dan gebruikt Leverancier alleen certificaten welke zijn verstrekt door de Opdrachtgever. Opdrachtgever ondersteunt geen wildcard certificaten die door de Leverancier of andere 3de partij zijn aangeschaft. - EIS
3. Machine to machine certificaten, die worden gebruikt voor het uitwisselen van gegevens onderling tussen machines, die door de Leverancier worden aangeschaft en gebruikt, krijgen per koppeling een certificaat en dit mag geen wildcard certificaat zijn. – EIS
4. De Leverancier is verantwoordelijk voor de aankoop van certificaten. Tenzij het gaat om de door Opdrachtgever beheerde domeinnamen. – EIS

3.3.6 Documentatie

1. Naast de verplichte documentatie die in Artikel 5 en 11 in de GIBIT worden gesteld houdt de Leverancier actuele overzichten, documentatie en handleidingen bij en stelt deze beschikbaar aan Opdrachtgever met minimaal de volgende eigenschappen:
    - Handleiding tbv het vervangen van certificaten gebruikt door de ICT Prestatie
    - Een overzicht van de parametrisering van de ICT Prestatie
    - Een overzicht van de noodzakelijke protocollen, services en accounts

    In de ontwerpdocumentatie stelt Opdrachtgever het volgende:
    - Gebruikte http-requestmethoden (GET, POST)
    - Informatie in de http-headers die voor het functioneren van belang zijn
    - Poorten en protocollen van en naar de Programmatuur zijn vastgelegd, dit mag in de vorm van een overzicht of netwerktekening
    - Procedure tbv (disaster) recovery – EIS

3.3.7 Onderhoud

1. De ICT Prestatie zit minimaal 5 jaar in de life cycle. Gedurende de looptijd van het contract wordt dit volledig ondersteund en is er technical support aanwezig. Enkel de laatste 2 versies van het Operating systeem en LTS versies die nog vallen in de 5 jaar life cycle worden ondersteund. – EIS
2. Patchmanagement wordt procesmatig en procedureel zodanig uitgevoerd, dat van de gebruikte code tijdig vanuit (externe) bibliotheken informatie wordt ingewonnen over technische kwetsbaarheden, zodat tijdig de laatste (beveiligings)patches kunnen worden geïnstalleerd. De Leverancier update tijdig zelf de ICT Prestatie en stelt hiervan de Opdrachtgever vooraf en achteraf op de hoogte. In overleg kan de Opdrachtgever zelf of samen met de Leverancier de updates uitvoeren nadat deze door de Leverancier hierover is ingelicht, mits er een duidelijke handleiding/instructies en ondersteuning van de Leverancier aanwezig is. Indien dit niet beschikbaar is blijft de Leverancier verantwoordelijk voor het patchmanagement. – EIS

3.3.8 Security

1. De ICT Prestatie blijft voldoen aan de meest actuele NCSC richtlijnen voor wat betreft de ICT-beveiligingsrichtlijnen voor webapplicaties, TLS, Mobile apps en HTTPS tijdens de looptijd van de Overeenkomst. https://www.ncsc.nl/ - EIS

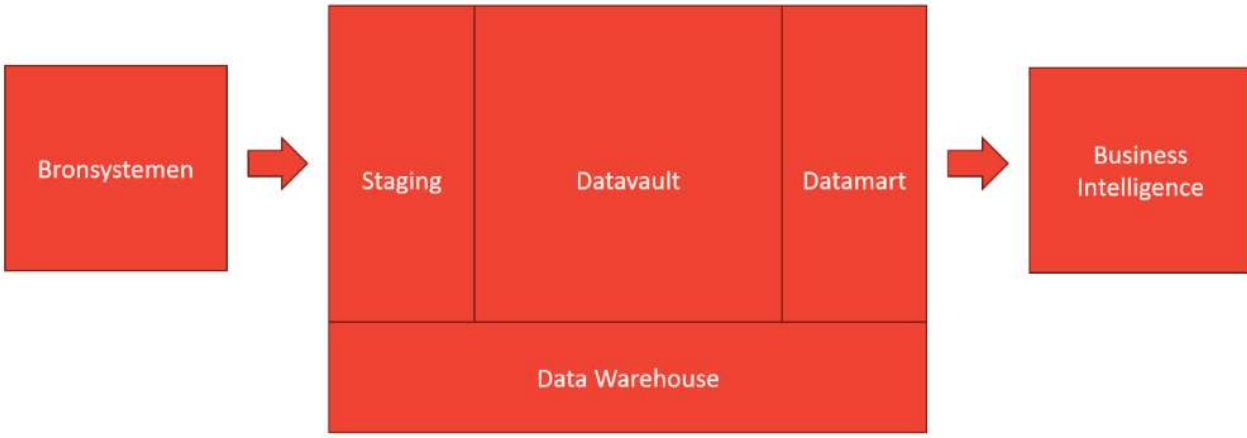
2. De ICT prestatie verzendt geen telemetrie naar de Leverancier welke niet is vastgelegd in de documentatie van deze aanbesteding. Indien door wijzigingen in de ICT Prestatie (updates, nieuwe functionaliteiten, etc) de inhoud van de telemetrie verandert, mag dit enkel worden verzonden naar de Leverancier na schriftelijke goedkeuring door de Opdrachtgever. De Leverancier stemt in dat deze veranderingen met de Opdrachtgever vooraf schriftelijk wordt afgestemd. - EIS
3. ESB verbindingen verlopen via een 2-way SSL handshake met een Signed Named SSL certificaat (geen self signed en/of wildcard certificaten). – EIS
4. De SSL Cipher Suites volgorde is zo ingesteld dat deze als eerste gebruik maakt van het sterkste Cipher en zo aflopend. Hierbij gebruikt de Leverancier enkel ciphers met de status goed en/of voldoende van het NCSC. – EIS
5. Onprem to SaaS, Saas to Onprem en SaaS to SaaS koppelingen verlopen altijd via de door Opdrachtgever aangeboden Enterprise Service Bus of de toekomstig aangeboden API Gateway. Tenzij het gaat om openbaar te raadplegen data, deze data mag rechtstreeks bij de aanbieder van de data worden geraadpleegd en/of opgehaald. – EIS
6. Encryptie & hashing algoritmes voldoen aan de nieuwste FIPS standaard. https://csrc.nist.gov/publications/fips – EIS

1. Security

1. Informatiebeveiliging wordt integraal meegenomen bij het ontwerp en de inrichting van applicatie en infrastructuur. – EIS
2. De leverancier moet zorg dragen voor een erkende en recente TPM verklaring afgegeven door een geregistreerde auditor. – EIS
3. Er mogen geen vertrouwelijke gegevens in cookies worden opgeslagen. Gebruik unieke namen, paden en domeinen voor cookies ten behoeve van authenticatie. – EIS
4. Sessies dienen na een bepaalde tijd te verlopen afhankelijk van de kriticiteit van de applicatie. – EIS

4. Architectuur en koppelingen

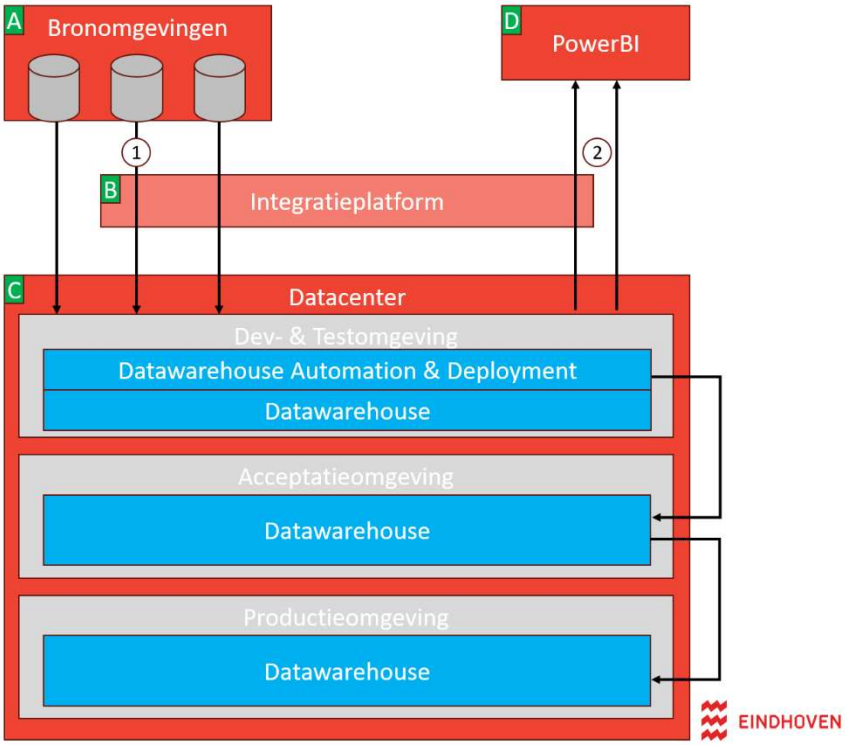
Dit hoofdstuk beschrijft de informatievoorziening van gemeente Eindhoven en de architectuureisen waaraan het datawarehouse automatiseringssysteem moet voldoen. Dit dient om de integratie met de informatievoorziening mogelijk te maken. Onderstaande afbeelding is de grafische weergave van de relevante omgevingen en de daarbij behorende koppelingen op hoofdlijnen. Bij iedere omgeving is een letter geplaatst en bij iedere koppeling een nummer, deze worden hieronder toegelicht.



Het Data Warehouse moet minstens voldoen aan de vereisten zoals de GEMMA referentiearchitectuur deze stelt. De volgende referentiecomponenten zijn relevant voor deze aanbesteding:

Referentiecomponent	Omschrijving
Data-laad en transformatiecomponent	Component voor het laden, controleren en transformeren van data naar een centraal datawarehouse inclusief mogelijkheden voor handmatige invoer.
Data-warehousecomponent	Component om actuele en historische gegevens gestructureerd op te slaan voor analyses en rapportages.
Managementinformatiecomponent	Component voor het ontwikkelen, publiceren en uitvoeren van managementanalyses en rapportages.

In algemene zin geldt dat de leverancier aansluit bij de GEMMA architectuur, de Common Ground architectuur en de Haven architectuur.



4.1. Omgevingen

Bovenstaand diagram bevat de volgende omgevingen:

A. Bronomgevingen

Dit kan zowel gaan om on-premise als SaaS-systemen waarvan de gegevens uitgelezen worden.

B. Integratieplatform

Veel geautomatiseerde gegevensuitwisseling tussen applicaties en databronnen verloopt via het integratieplatform van de gemeente Eindhoven. Per koppeling zal de afweging gemaakt moeten worden of deze inderdaad via dit platform dient te verlopen, of dat er direct aan het datawarehouse gekoppeld kan worden. Het integratieplatform faciliteert verscheidene subsystemen, zoals een Enterprise Service Bus (ESB) en een API-Manager.

C. Datacenter

Het datacenter van de gemeente Eindhoven, locatie High Tech Campus (HTC). Dit is een Tier 4 colocation datacenter van NorthC voor optimale veiligheid en beschikbaarheid. Het datacenter biedt toegang tot een groot aantal nationale en internationale clouddiensten en -providers en beschikt over 24/7/365 on-site beveiliging.

Door de hoge BIV-classificering van de te gebruiken gegevens dient dit systeem in een eigen datacenter gehost te worden, en kan er (nog) niet naar een Cloud-oplossing worden toegewerkt.

D. PowerBI

Krachtige en gebruiksvriendelijke dashboarding-applicaties te realiseren door middel van PowerBI.

4.2 Koppelingen

Koppelingen uit bovenstaande afbeelding worden hier beschreven, volgens de nummering uit het diagram.

Koppelingen tussen systemen zijn noodzakelijk op het moment dat er gegevens van een bronsysteem gebruikt moeten worden in het doelsysteem. De gewenste gegevens uit dit bronsysteem moeten dan beschikbaar worden gemaakt en vervolgens op een veilige manier worden getransporteerd naar het doelsysteem waarin de gegevens geïntegreerd worden opgenomen.

Patronen

Per koppeling geldt het volgende:

Om het transport van de data van het bronsysteem naar het doelsysteem, of andersom, mogelijk te maken kan uit twee patronen gekozen worden:

1. Database-koppeling (native dan wel generiek) (eis)
    a. Oracle
    b. MS SQL
    c. PostgreSQL
2. Importeren van bestanden (Lokaal/Netwerkshare) (CSV, XLS(X)) (eis)
    a. Automatische imports: Imports moeten geautomatiseerd plaats kunnen vinden.
    b. Manuele agendering: In-/Uitschakeling imports, agendering van imports, en configureren van locaties moet handmatig gedaan kunnen worden.

Het is belangrijk dat beide patronen gerealiseerd kunnen worden.

Andere patronen kunnen zijn:

3. Database-koppelingen met andere database-soorten.
4. Beveiligde bestandsoverdracht (SFTP).
5. Het kunnen importeren van andere bestandstypen.
6. Inlezen gegevens via API-koppeling (evt. via standaard connector).

Koppeling 1: Bronsysteem → Datawarehouse

Doel	De gemeente Eindhoven wil over een keur aan gegevens uit diverse bronsystemen kunnen beschikken. Hierdoor wordt het mogelijk om deze gegevens samen met gegevens uit andere bronnen te combineren. Uitgangspunt is dat de gegevens minimaal 1 keer per dag in het dataplatform beschikbaar komen, om dagelijks bijgewerkte rapportages te kunnen realiseren.
Patroon	Hier moet afhankelijk van de bron ofwel direct gekoppeld kunnen worden met de database (patroon 1) ofwel via gegevensoverdracht via bestanden (patroon 2).
Toe te passen standaard	Afhankelijk van specifiek bronsysteem. Te beschrijven in implementatieplan.
Technische realisatie	Afhankelijk van specifiek bronsysteem. Te beschrijven in implementatieplan. De gegevens moeten altijd via een beveiligde connectie worden uitgewisseld.