



Rijksinkoop samenwerking
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Project Startarchitectuur (PSA)

Rijksinkoop samenwerking

Bezoekadres

Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

Bijlage D

Databeheer LMVW

Europese aanbesteding
Openbare procedure

voor het

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De directie Woningbouw

Datum	15 juli 2026
Kenmerk	201865002.345.003
Versie	1.0

Managementsamenvatting

De directie Woningbouwbeleid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is beleidsmatig verantwoordelijk voor het terugdringen van het tekort aan woningen in Nederland. Om inzicht te verkrijgen hoeveel woningbouwplannen worden gemaakt en gerealiseerd, bestaat er door samenwerking tussen de Vereniging Nederlandse Gemeenten (VNG), het Interprovinciaal Overleg (IPO) en BZK een Landelijke Monitor Voortgang Woningbouw (LMVW).

De huidige LMVW

De huidige LMVW wordt gekenmerkt door versnipperde dataopslag, beperkte datakwaliteit, hoge administratieve lasten en moeizame ontsluiting van gegevens. Knelpunten die worden ervaren zijn dat data op verschillende manieren (digitaal, Excel lijsten, etc.) wordt aangeleverd en dat hierdoor de datakwaliteit en volledigheid van gegevens te wensen over laat. Door dit laatste is ook de betrouwbaarheid van de gepresenteerde informatie in het geding. Een deel van de gegevens is vertrouwelijk en door deze beperkte datakwaliteit worden kunnen vertrouwelijke gegevens ongewenst openbaar gemaakt worden. Verder ervaren gemeenten hoge administratieve lasten om de gegevens aan te leveren.

Ambities van de LMVW

De presentatie van de woningbouwplannen van gemeenten in de vernieuwde LMVW moet bijdragen aan:

- Een betere interbestuurlijke samenwerking tussen gemeenten, provincies en Rijk
- Eerder en meer inzicht in ruimtelijke knelpunten op de woningbouw
- Inzicht in daadwerkelijke realisaties en latere bewoning van woningbouwplannen
- Betere besluitvorming en zodoende een versnelling van de woningbouw
- Transparantie richting burgers en parlement

Processen, diensten en informatiestromen

Om de knelpunten aan te pakken en de doelen vorm en inhoud te geven zijn in eerste instantie de processen, diensten en informatiestromen rondom de LMVW in kaart te gebracht en is een informatie objectenmodel (binnen VRO ook wel datamodel genoemd) opgesteld. Dit betekent dat:

- Het proces is op hoofdlijnen gemoduleerd, verdeeld in verschillende EPICS en vertaald naar functionaliteiten in de vorm van user story's.
- De informatieobjecten zijn uitgewerkt in een UML-model.
- De gebruikte informatieobjecten zijn geclassificeerd en in termen van informatiebeveiliging zijn doorvertaald naar maatregelen, waarbij vooral de integriteit van de gegevens van belang bleken te zijn.

Daarna zijn er niet-functionele eisen in de vorm van user story's t.a.v. de LMVW opgesteld en zijn de meest belangrijke kaders van uit wet- en regelgeving en voorschriften benoemd.

Additionele bronnen met aanvullende gegevens

Dit betreft het uitvragen van aanvullende gegevens bij overige beschikbare bronnen (BAG, DSO, LVBB, BRK en het CBS). Het combineren van de woningbouwplannen met deze aanvullende gegevens uit overige bronnen is in hoofdlijnen om:

- Te duiden welke mijlpalen binnen het planproces zijn bereikt op planniveau.
- Te duiden welk (type) woningen daadwerkelijk zijn gerealiseerd.
- Te duiden welk type huishoudens er in welk type plan terecht komen.
- Om de administratieve last van monitoringstaken te verminderen door de monitoringslast niet als (nieuwe) uitvragen bij de gemeente of provincie neer te leggen.

Dashboard met WOBI-gegevens

Tot slot is ook gebleken dat de LMVW een goed platform kan zijn voor een publiek dashboard voor het actief presenteren van informatie van woningbouwprojecten die een financiële bijdrage van het

Rijk ontvangen. Het dashboard wordt gepresenteerd als interactieve kaart van projecten op gemeenteniveau in Nederland.

Applicatielandschap

Tot slot is er nog een Archimate visualisatie gemaakt van het applicatielandschap, waarbij o.a. ook de belangrijkste koppelvlak in kaart zijn gebracht. Tevens is er met Digikoppeling standaard in de variant van REST API's voorgesorteerd op de bij de overheid geldende open standaard voor informatie-uitwisseling.

1. De Landelijke Monitor Voortgang Woningbouw

De Landelijke Monitor Voortgang Woningbouw (LMVW) is het centrale instrument voor het monitoren en sturen van de woningbouwopgave in Nederland. De LMVW is ontstaan uit een interbestuurlijke samenwerking tussen de VNG, het IPO en het ministerie van BZK en voorziet in de behoefte om landelijk inzicht te krijgen in de voortgang van woningbouw en te kunnen sturen op beleidsdoelen. De monitor bevat woningbouwplannen met hun locatie, plankenmerken en woningkenmerken die volgens gemeenten in voorbereiding of uitvoering zijn. Deze gegevens moeten tevens worden verrijkt met landelijke databronnen.

1.1. Het maatschappelijk belang

Het terugdringen van het tekort aan woningen blijft één van de grootste prioriteiten van deze tijd. De schrijnende verhalen van mensen die stappen in hun leven moeten uitstellen, vanwege het gebrek aan passende huisvesting benadrukken dit. De spanning op de woningmarkt en de verwachte huishoudensgroei blijft groot. De leeftijd waarop jongvolwassenen het ouderlijk huis verlaten is verder gestegen. De presentatie van de woningbouwplannen van gemeenten in de vernieuwde LMVW moet bijdragen aan een betere beleidsbesluitvorming, versnelling van woningbouw, verbeterde samenwerking tussen overheden en transparantie richting burgers en het parlement.

1.2. Voldoende woningbouwplannen

Gelukkig zijn er voldoende woningbouwplannen. Maar deze plannen moeten wel gerealiseerd worden. Om deze plannen te realiseren hebben betrokken partijen op de Woontop hun handtekening gezet onder gezamenlijke afspraken. Op deze manier wordt gewerkt aan de realisatie van 100.000 woningen per jaar. Het woningtekort is echter nog steeds te hoog (4,8%), waarbij een tekort van 2% wordt gezien als een situatie waarbij er sprake is van een normale spanning op de woningmarkt. Rekening houdend met de verwachte huishoudensgroei en de sloop van woningen wordt bij een realisatie van 100.000 woningen per jaar in 2034 het evenwichtige niveau van 2% bereikt. Kortom: de opgave is en blijft groot¹.

Dit benadrukt de urgentie om op nationaal niveau vast te houden aan de koers die nodig is om 100.000 woningen per jaar te realiseren. Daarvoor is en blijft het nodig dat het woon- en woningbouwbeleid optimaal bijdraagt aan de gewenste stabiliteit, voorspelbaarheid en continuïteit van deze opgave.

Momenteel duurt de ontwikkeling en realisatie van een woningbouwproject gemiddeld 10 jaar. Woningbouwplannen kunnen vertraging oplopen of niet doorgaan. Om die reden is met lokale overheden afgesproken dat er 30% meer plancapaciteit beschikbaar moet zijn dan de bouwopgave. Voor de periode 2025 tot en met 2030 (looptijd huidige woondeals) is de geraamde bruto plancapaciteit 930.400 woningen (127%). Een punt van zorg is dat een groot deel van deze plannen nog niet hard is. Om de afspraken t/m 2030 te kunnen nakomen moet er gewerkt worden aan het hard maken van de woningbouwplannen en het vergunnen ervan.

¹ Kamerbrief Aanbieding rapporten Primos 2025_ Landelijke Monitor Voortgang Woningbouw en Woningdelers

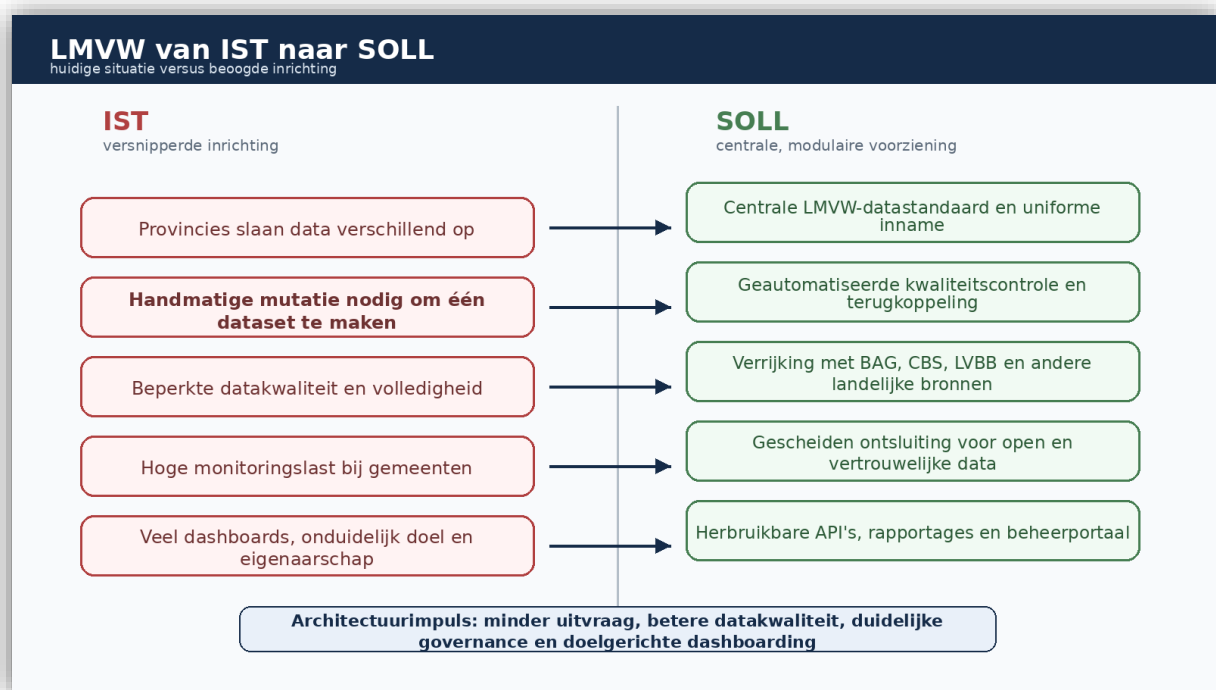
De LMVW is in samenwerking tussen het Rijk, provincies en gemeenten ontwikkeld tegen de achtergrond van de benoemde grote woningbouwopgave in Nederland en moet op basis van indicatoren en ontwikkelingen inzicht geven op de gestelde doelstellingen van 100.000 woningen per jaar worden gerealiseerd. Met dit inzicht:

- Worden alle woningbouwplannen landelijk in beeld gebracht (in voorbereiding en uitvoering, inclusief locatie en kenmerken);
- Kan worden gevolgd of er landelijk en regionaal voldoende plancapaciteit is om de bouwdoelen te halen;
- Kan worden gestuurd op de voortgang en uitvoering van de woondeals;
- Kunnen plannen beleidsmatig worden bijgesteld of herijkt.

1.3. De LMVW lost knelpunten op

De huidige situatie wordt gekenmerkt door versnipperde dataopslag, beperkte datakwaliteit, hoge administratieve lasten en moeizame ontsluiting van gegevens. Knelpunten die worden ervaren zijn:

- Data worden op verschillende manieren opgeslagen en aangeleverd;
- Datakwaliteit en volledigheid zijn onvoldoende;
- Gemeenten ervaren hoge administratieve lasten;
- Data is moeilijk toegankelijk voor afnemers.



Figuur 1 Knelpunten in de huidige werkwijze vs. de gewenste werkwijze²

Dit belemmert effectieve beleidssturing en transparantie. Door de LMVW te stroomlijnen en gegevensaanlevering te digitaliseren, wordt één landelijk, uniform overzicht van woningbouwplannen verkregen en wordt het mogelijk om op de voortgang te sturen. In de huidige situatie is er een gebrek aan inzicht, verschillen in data en het gat tussen plannen en daadwerkelijke bouw. Met één landelijk, uniform overzicht van woningbouwplannen probeert de LMVW twee kernproblemen op te lossen:

1. Een gebrek aan uniformiteit voor interbestuurlijke sturing en landelijke analyses

² Project start architectuur (PSA) Landelijke Monitor Voortgang Woningbouw (LMVW), versie 0.1, maart 2026, Robin Vink

- Op dit moment worden gegevens niet altijd conform de afgesproken definities verzameld, opgeslagen of aangeleverd vanuit provincies (en dus ook richting provincies vanuit gemeenten). Hierdoor worden uitgevraagde attributen verkeerd geïnterpreteerd en is er semantische verwarring over de aangeleverde gegevens. Dit met het gevolg dat de datakwaliteit matig is.
 - Daarnaast is er variëteit aan in welke vorm de gegevens worden aangeleverd. Soms Excel-bestanden via email, soms via digitale koppelingen. Hierdoor is een landelijke vergelijking lastig te maken. Foutieve invoer van data (zoals o.a. negatieve getallen waar dit niet mogelijk is) worden gewoon aangeleverd.
 - Het is belangrijk dat gemeenten, provincies en Rijk hetzelfde, uniforme beeld hebben. Dit geeft inzicht in knelpunten. Door de monitor meer te structureren en digitaliseren worden de afgesproken uniforme definities afgedwongen. Dit maakt interbestuurlijke regionale en landelijke samenwerking rond de woningbouwopgave mogelijk. De datakwaliteit is op dit moment vaak te beperkt om regionaal of landelijk goed te kunnen sturen, verantwoording af te leggen of analyses naar knelpunten uit te kunnen voeren.
2. *Voldoende inzicht in doorlooptijden, daadwerkelijke realisatie en post-realisatie*
- Beperkingen in de datakwaliteit en de beperkte ambtelijke capaciteit om de monitoringslast te verzwaren zorgen voor een gebrek aan inzicht in de voortgang van woningbouwplannen. Verbeteringen in de datakwaliteit en digitalisering maken het mogelijk om gegevens uit bestaande landelijke gestructureerde databronnen te halen. Met name de BAG en het DSO bieden de mogelijkheid om processtappen in de planontwikkeling te volgen zonder aanvullende gegevens uit te vragen. Bij het CBS zijn gegevens beschikbaar over welke woningen daadwerkelijk gerealiseerd zijn en hoe deze kenmerking zich post-realisatie ontwikkelen. Zowel de methode van deze dataverrijking als de verkregen gegevens worden teruggekoppeld naar de gemeenten en provincies.

1.4. Het doel van de vernieuwde LMVW

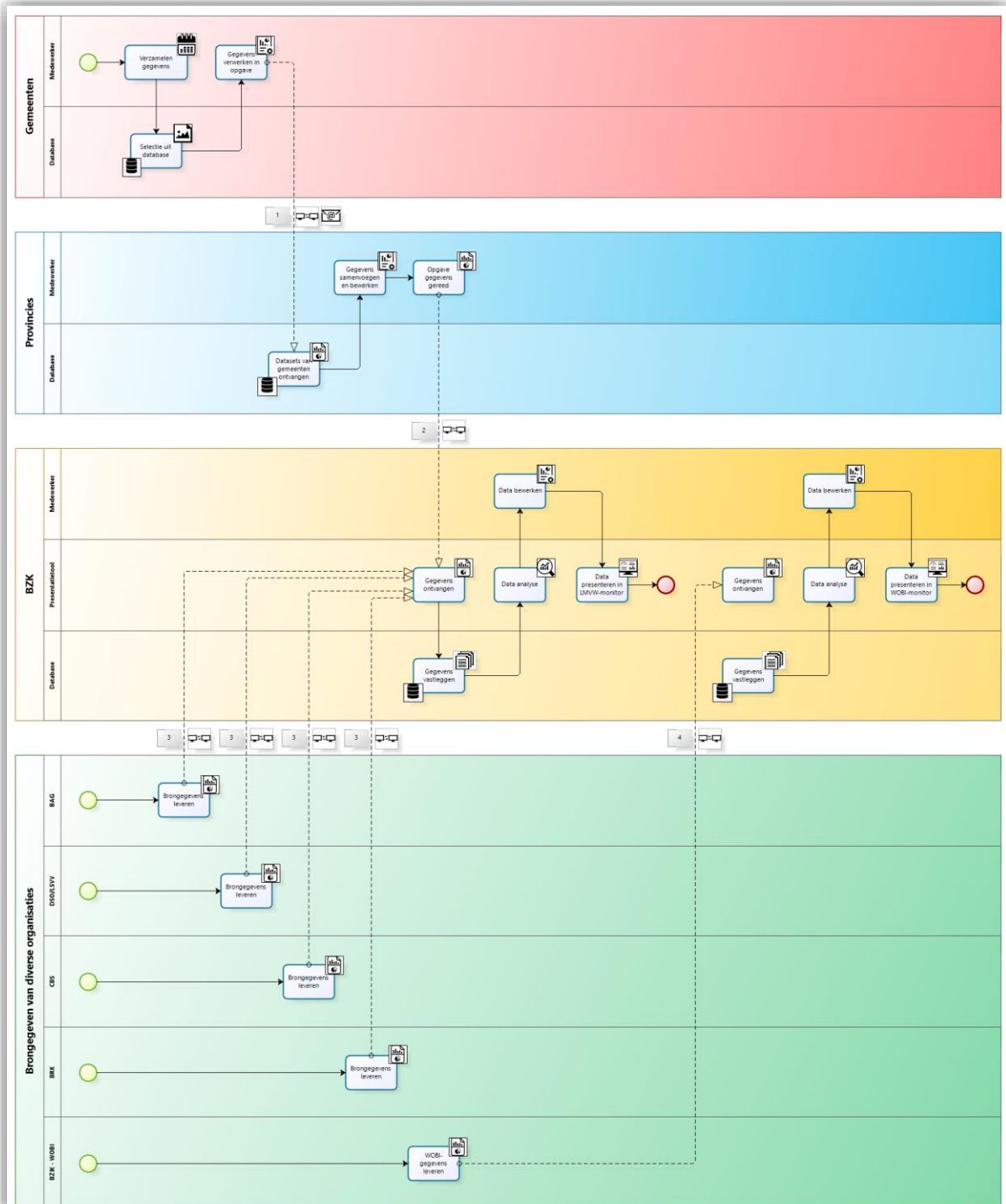
Het doel van de verandering aan de LMVW is het realiseren van een centrale, gestandaardiseerde en toekomstbestendige datavoorziening die de beleidssturing ondersteunt, de datakwaliteit verhoogt, de administratieve lasten verlaagt en de transparantie en hergebruik van data mogelijk maakt³. Om dit mogelijk te maken is het belangrijk dat de vernieuwde LMVW de volgende zaken levert:

- een centrale dataset met woningbouwplannen;
- geautomatiseerde dataverwerking en kwaliteitscontrole;
- integratie met bestaande databronnen;
- dashboards en rapportages;
- veilige toegang voor verschillende gebruikersgroepen.

³ Project start architectuur (PSA) Landelijke Monitor Voortgang Woningbouw (LMVW), versie 0.1, maart 2026, Robin Vink

2. Het proces van verzamelen van gegevens

In de onderstaande figuur is het proces van de uitvraag van de gegevens t.b.v. de LMVW beschreven. De figuur laat zien hoe iedere van de 342 gemeenten (2026) als bronhouder en verstrekker – na uitvraag door de provincie – de uitgevraagde gegevens zelf uit hun systemen verzamelen en doorsturen (**koppelvlak 1**) naar hun provincie als afnemer. Hoe deze gegevensuitwisseling verloopt, valt buiten het zicht van de LMVW. De door de gemeenten aangeleverde gegevens ondergaan bij de provincies een verwerking. Denk daarbij aan het verifiëren en valideren van de gegevens, controles op kwaliteit en betrouwbaarheid, het verrijken van gegevens vanuit een provinciale context, etc.



Figuur 2 Het proces van het verzamelen van gegevens t.b.v. de LMVW

Daarna worden de gegevens vanuit de provincie als verstrekker in opdracht van de directie VRO van het ministerie van BZK aangeleverd aan de LMVW (**koppelvlak 2**), alwaar ze worden gevalideerd, verwerkt en gepresenteerd in de LMVW.

Verder worden op basis van locatie/geometrie bij een aantal overige bronnen (BAG, DSO, LVBB, BRK en het CBS) aanvullende gegevens opgevraagd en geleverd (**koppelvlak 3**). Doel van de uitvraag is om:

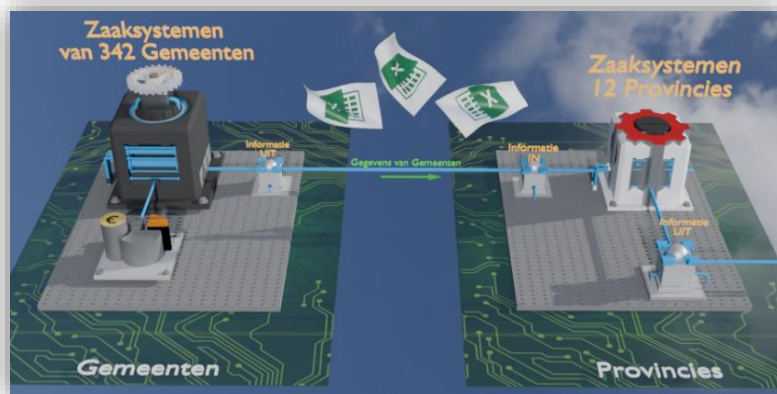
- Te duiden welke mijlpalen binnen het planproces zijn bereikt op planniveau.
- Te duiden welk (type) woningen daadwerkelijk zijn gerealiseerd.
- Te duiden welk type huishoudens er in welk type plan terecht komen (CBS).
- Om de administratieve last van monitoringstaken te verminderen door de monitoringslast niet als (nieuwe) uitvragen bij de gemeente of provincie neer te leggen. De monitoringslast kan voor gemeenten verder verminderen wanneer de verrijking lokaal bij de gemeenten plaatsvindt. In plaats van handmatig informatie verzamelen kan een deel van de planinformatie via het DSO, de LVBB, de BAG en de BRK verzameld worden. De ervaring die bij de LMVW wordt opgedaan willen we daarom open source beschikbaar stellen.

Tot slot worden er ook vanuit de WOBI gegevens brongegevens gepubliceerd via de voorziening die t.b.v. de LMVW (**koppelvlak 4**) wordt gerealiseerd. Doel van deze publicatie is dat BZK actief (volgens de Wet open overheid (Woo)) gegevens in een aparte WOBI-monitor publiek beschikbaar wil stellen. Voorsnog staan deze gegevens op zichzelf en los van de woningbouwplannen en gerealiseerde woningen in de LMVW. Wel is de LMVW een voorziening dat hiervoor goed hergebruikt kan worden. Aan de andere kant is het denkbaar dat deze gegevens in de toekomst voor analyse doeleinden mogelijk toch gecombineerd gaan worden met de gegevens van de woningbouwplannen en gerealiseerde woningen die al in de LMVW staan. Mocht dit opportuun worden, dan moet in een aanvullende DPIA vanuit privacy overwegingen opnieuw een beoordeling van de risico's plaatsvinden.

In de volgende paragrafen zijn de functionele eisen voortvloeiend uit dit proces als user story's verwoord in functionele eisen. De Epics 1, 2 (bij gemeenten en provincies) vallen buiten de LMVW, maar zijn volledigheidshalve voor de beeldvorming wel beschreven en uitgewerkt.

2.1. Verzamelen en doorsturen van woningbouwplannen naar provincies

Gemeenten registreren gegevens over woningbouwplannen t.b.v. hun eigen beleid, sturing en lokale verantwoording. Een deel van de gegevens over woningbouwplannen worden op verzoek van de provincie uit hun systemen verzameld en bij de provincies aangeleverd. Voor een deelverzameling van deze gegevens die op verzoek van de provincie worden verzameld door gemeenten zijn landelijk uniforme definities afgesproken via de LMVW. Deze deelverzameling moeten de provincies doorleveren t.b.v. de LMVW.



Figuur 3 Het verzamelen van gegevens door gemeenten en het doorsturen naar provincies

Gemeenten zijn eigenaar van de brongegevens en daarmee verantwoordelijk voor de kwaliteit van de gegevens. Dit is in de volgende Epics en user story verwoord als functionele eis.

Epic 1 – Het verzamelen van de woningbouwplannen door gemeenten:

ID	Als	Wil ik	Zodat
Epic.01	gemeente	De uitgevraagde gegevens over woningbouwplannen t.b.v. de LMVW uit mijn systemen kunnen halen,	Deze gegevens opgestuurd kunnen worden naar de provincie waarin mijn gemeente zich bevindt.
Input van de User Story:		Resultaat van de User Story:	
Uitvraag van de gegevens over woningbouwplannen t.b.v. de LMVW.		De uitgevraagde gegevens over woningbouwplannen t.b.v. de LMVW.	
Betrokken voorzieningen:		De Planmonitorsystemen van de gemeenten.	

Tabel 1 Epic 01: Het verzamelen van de woningbouwplannen door gemeenten.

Bij deze Epic behorende user story's zijn:

ID	Als	Wil ik	Zodat
Epic.01/ US.01	gemeente	De door BZK uitgevraagde gegevens over woningbouwplannen t.b.v. de LMVW uit mijn systemen kunnen halen,	Deze gegevens digitaal of als een bestand (bijvoorbeeld in Excel) opgestuurd kunnen worden naar de provincie waarin mijn gemeente zich bevindt.
Epic.01/ US.02	gemeente	De verzamelde gegevens digitaal of als een bestand (bijvoorbeeld in Excel) kunnen opsturen naar de provincie waarin mijn gemeente zich bevindt,	De provincie de gegevens in hun eigen systemen kan vastleggen en bewerken/verrijken.

Tabel 2 User Story's bij Epic 01: Het verzamelen van de woningbouwplannen door gemeenten.

2.2. Het in opdracht van BZK Ontvangen, bewerken en doorsturen van gegevens t.b.v. de LMVW

Iedere provincie ontvangt de gegevens van de woningbouwplannen van alle in de provincie gelegen gemeenten en verwerkt deze gegevens. De provincie controleert de gegevens op volledigheid, geldigheid, inconsistenties, plausibiliteit, duplicering en uniformeert waar nodig de gegevens in een provinciaal planmonitoringssysteem. De deelverzameling die de provincie t.b.v. de LMVW ontvangt van de gemeenten wordt geleverd aan de landelijke dataset van de LMVW conform het format en geldende definities van de Basisset 2.0.



Figuur 4 Het ontvangen en verwerken van de gegevens door provincies

Provincies en/of gemeenten hebben soms behoefte aan gedetailleerdere gegevens dan vanuit de LMVW wordt gevraagd. Het kan het zijn dat er mapping moet plaatsvinden, bijvoorbeeld bij een extra onderverdeling van prijssegmenten of planologische status, naar de onderverdeling in de landelijke Basisset. Deze mapping vindt plaats op provinciaal niveau en moet gecontroleerd worden.

Epic 2 – Het ontvangen en verwerken van de gegevens door provincies:

ID	Als	Wil ik	Zodat
Epic.02	provincie	De door de gemeenten opgestuurde gegevens over woningbouwplannen t.b.v. de LMVW kunnen ontvangen in mijn systemen,	Ik deze gegevens kan analyseren, beoordelen (op o.a. vertrouwelijkheid), verwerken, verrijken en kan opsturen naar BZK voor opname in de LMVW.
Input van de User Story:		Resultaat van de User Story:	
De gegevens over woningbouwplannen van gemeenten t.b.v. de LMVW.		De gegevens over woningbouwplannen van de provincie verzonden naar BZK t.b.v. de LMVW.	
Betrokken voorzieningen:			
De zaaksystemen van de gemeenten.		Het zaakstelsysteem van iedere provincie.	

Tabel 3 Epics 02: Het ontvangen en verwerken van de gegevens door provincies.

Bij deze Epic behorende user story's zijn:

ID	Als	Wil ik	Zodat
Epic.02/ US.01	provincie	De gegevens van woningbouwplannen van alle in mijn provincie gelegen gemeenten kunnen ontvangen,	Ik deze gegevens in mijn systemen kan vastleggen.
Epic.02/ US.02	provincie	De van de gemeenten ontvangen gegevens kunnen analyseren, beoordelen (op o.a. vertrouwelijkheid), verwerken en verrijken,	Ik een geverifieerde en gevalideerde set van gegevens aan BZK kan toesturen.

Tabel 4 User Story's bij Epic 03: Het doorsturen van de gegevens door provincies.

2.3. Het in opdracht van BZK ontvangen en verwerken van de gegevens in de LMVW

Nadat iedere provincie de gegevens heeft gecontroleerd en verwerkt, dan wordt de geverifieerde set aan gegevens over woningbouwplannen verstuurd naar de landelijke dataset. De technische oplossing biedt de mogelijkheid om aan te leveren via een API of via een bestandsupload. Dit is het eerste onderdeel van de op te leveren voorziening.

Provincies beschikken over eigen systemen om woningbouwplannen te registreren. Niet alle provinciale aanleveringen worden volgens geldende definities uit Basisset 2.0 of juiste structuur van het format aangeleverd. Onderdelen van gegevens die vaak ontbreken of afwijken van de Basisset zijn:

- Bestanden zijn aangeleverd in afwijkende GIS-projecties.
- Bestanden zijn aangeleverd in ander format met afwijkende kolomnamen en bijvoorbeeld afwijkende prijsklassen of fasering.
- Het ontbreken van polygonen in een nieuwe levering, terwijl dit eerder wel het geval was.
- Invoerfouten, lege velden en totalen woningen die niet aansluiten.
- Sterke afwijkingen tussen opeenvolgende aanleveringen.

Voor het beheer van de landelijke dataset moeten een aantal acties worden uitgevoerd op de aangeleverde data:

- Aangeleverde gegevens moet gecontroleerd worden op juiste bestandsformaat en structuur en het aangeleverde format (kolommen en categorieën) moet voldoen aan het gegevensmodel. Deze controle vindt automatisch plaats en wordt teruggekoppeld aan de provincie met verzoek voor een correctie.
- Verantwoordelijkheid van de datakwaliteitscontrole ligt primair bij de gemeenten en provincies. Opdrachtnemer voert nog een laatste controle uit op volledigheid, geldigheid, inconsistenties, plausibiliteit en duplicaten via een geautomatiseerde datacontrole. Deze controle vindt automatisch plaats en wordt teruggekoppeld aan de provincie met verzoek voor een correctie of aanvulling indien dat nodig is.
- Mapping van de gegevens in de provinciale systemen naar het gegevensmodel van de LMVW: Deze mapping is door de provincie of gemeente gemaakt, maar fouten hierin kunnen wordenesignaleerd door de beheerder. Daarnaast kan er mapping nodig zijn bij historische gegevens na wijziging van het gegevensmodel.

Daarnaast wordt een samenvattende rapportage gegenereerd ter signalering aan BZK en wordt deze meegenomen bij het maken van rapportages aan de Kamers.

Epic 3 – Het ontvangen en beoordelen van de gegevens door BZK:

ID	Als	Wil ik	Zodat
Epic.03	BZK	De ontvangen sets van gegevens over woningbouwplannen van de 12 provincies vastleggen en t.b.v. de LMVW kunnen: • Analyseren; • Beoordelen op semantiek, datakwaliteit en uniformiteit,	Ik weet dat ik over een betrouwbare set aan gegevens beschik die ik kan presenteren in de LMVW.
Input van de User Story:		Resultaat van de User Story:	
• De gegevens over woningbouwplannen van provincies t.b.v. de LMVW.		• Een geverifieerde set aan gegevens over woningbouwplannen in Nederland.	
Betrokken voorzieningen:			
• Het zaakstelsel van iedere provincie.		• De database met woningbouwplannen t.b.v. de LMVW.	

Tabel 5 Epic 03: Het ontvangen en beoordelen van de gegevens door BZK.

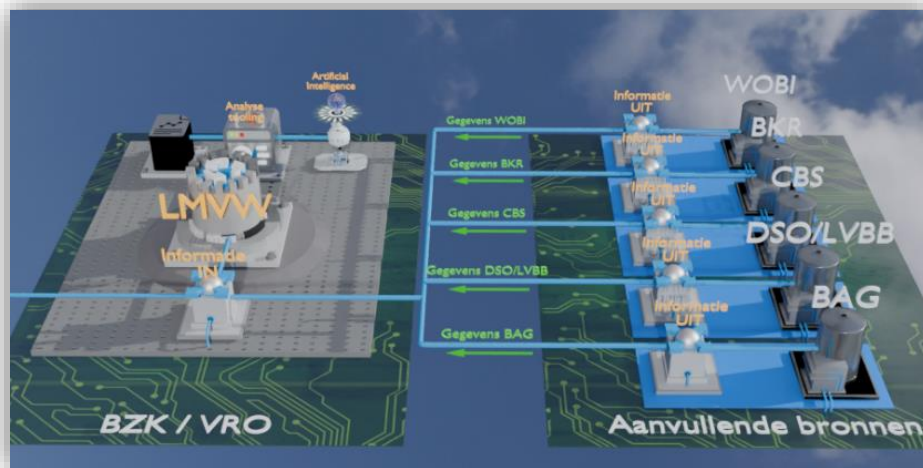
Bij deze Epic behorende user story's zijn:

ID	Als	Wil ik	Zodat
Epic.03/ US.01	BZK	Via een digitale koppeling minimaal twee dataleveringen door provincies per jaar kunnen faciliteren en verwerken,	Ik de LMVW twee keer per jaar kan bijwerken en verschillende rapportages kan maken voor o.a. gemeenten en provincies.
Epic.03/ US.02	BZK	De ontvangen sets van gegevens over woningbouwplannen van iedere provincie in de LMVW kunnen vastleggen,	Ik deze gegevens vanuit de LMVW kan analyseren en beoordelen op semantiek, datakwaliteit en uniformiteit.
Epic.03/ US.03	BZK	De actuele plannen, vervallen plannen, gerealiseerde plannen en historische plangegevens/aanleveringen aan elkaar kunnen koppelen met een uniek ID,	Historische analyses op basis van de LMVW-data makkelijker uit te voeren zijn.
Epic.03/ US.04	BZK	Dat de dataleveringen van de provincies worden bewaard,	Er een historische database ontstaat en historische analyses kunnen worden gedaan op de woningbouw door de tijd (tijdreizen) heen.
Epic.03/ US.05	BZK	Dat de aangeleverde gegevens worden gecontroleerd op volledigheid, geldigheid, inconsistenties, duplicaten en plausibiliteit,	De stuurgroep van de LMVW geïnformeerd kan worden over de datakwaliteit.
Epic.03/ US.06	BZK	Dat de technische oplossing de herkomst van alle data opslaat: organisatie, softwaresystemen gemeente en provincie, extractiedatum,	De stuurgroep LMVW geïnformeerd kan worden over de dataketen
Epic.03/ US.07	BZK	Dat Opdrachtnemer voorziet in vaste aanspreekpunten voor stuurgroep LMVW en provincies bij aanlevering, correctie en verwerken van provinciale gegevens,	Problemen en oplossingen snel gesignaleerd en opgepakt kunnen worden.

Tabel 6 User Story's bij Epic 03: Het ontvangen en beoordelen van de gegevens door BZK.

2.4. Het ontvangen en verwerken van de gegevens uit landelijke voorzieningen en het DSO

Het verzamelen van gegevens uit andere bronnen is het tweede deel van de te leveren voorziening. Met de gebiedsmarkering (polygoon/geometrie) die via de provinciale aanlevering is ontvangen kunnen gegevens worden opgehaald uit de BAG, het DSO/LVBB, de BRK.



Figuur 5 Het ontvangen van de gegevens uit overige bronnen

De verrijking van deze gegevens gebeurt bij voorkeur al lokaal bij de gemeente. Om de vraag naar ambtelijke capaciteit voor monitoring te verminderen en omdat niet iedere gemeente daar een geschikt systeem voor heeft starten we met een centrale oplossing. De gemaakte softwarematige oplossingen en toegepaste beslisregels om de nodige gegevens uit de BAG, DSO/LVBB, BRK te halen worden zoveel mogelijk open source beschikbaar gesteld. Dit verlaagt de drempel om deze bronnen lokaal te gebruiken.

Het gebruik maken van de landelijke voorzieningen vraagt veel van de datakwaliteit van de provinciale aanleveringen. Ook verwachten we dat de interpretatie en juiste toepassing van de gegevens uit de landelijke voorziening ontwikkeltijd vraagt.

Het is denkbaar dat met gebruik van tekstanalyse (NLP/AI) om niet gestructureerde bronnen als omgevingsdocumenten, planregels, publicatieteksten van bekendmakingen, raadsstukken, college besluiten, uitspraken RvS en uitspraken rechtspraak uit te lezen en te duiden. Hoewel het kansrijk lijkt om gegevens uit deze bronnen te halen zijn ze momenteel van beperkte toegevoegde waarde boven op de informatie die uit gestructureerde bronnen als de BAG, de BRK, onderdelen van het DSO en bij het CBS vandaan te halen zijn. Na het verrijken van de woningbouwplannen via de koppeling tussen locatiegegevens uit gestructureerde bronnen zien we de mogelijkheid om het toepassen van tekstanalyse verder te verkennen.

Epic 4 – Het ontvangen van aanvullende gegevens uit overige bronnen:

ID	Als	Wil ik	Zodat
Epic.04	BZK	Op basis van de plangeometrie uit de provinciale aanlevering sets van gegevens uit overige bronnen (BAG, DSO, LVBB, BRK en het CBS) kunnen ontvangen en toevoegen aan de LMVW,	Ik de al uitgevraagde set van gegevens van gemeenten/provincies met deze aanvullende gegevens uit landelijke databronnen kan verrijken.
Input van de User Story:		Resultaat van de User Story:	
Aanvullende gegevens van gerelateerde databronnen (BAG, DSO, LVBB en BRK) t.b.v. de LMVW.		Een verrijkte set aan gegevens over woningbouwplannen en gerealiseerde woningen in Nederland.	

Betrokken voorzieningen:

- De systemen voor het ontsluiten van databronnen (BAG, DSO, LVBB, BRK).
- Een verrijkte database met woningbouwplannen en gerealiseerde woningen t.b.v. de LMVW.

Tabel 7 Epic 04: Het bewerken van gegevens en data-analyse op de LMVW-database

Bij deze Epic behorende user story's zijn:

ID	Als	Wil ik	Zodat
Epic.04/ US.01	BZK	Dat de technische oplossing registreert op basis van de plangeometrie uit de provinciale aanlevering binnen en buiten plannen BAG gegevens van verblijfsobjecten met woonfunctie en bijhorende panden. Met name relevante gegevens uit de BAG zijn aantallen verblijfsobjecten, panden, IDs van de verblijfsobjecten en panden, statussen en statusmutaties, brondocumenten,	• De LMVW kan worden aangevuld met aantallen vergunde, in aanbouw zijnde, gerealiseerde of gesloopte woningen per plan. • De LMVW kan worden aangevuld met behaalde mijlpalen binnen een plan en het moment daarvan, zodat doorlooptijden kunnen worden berekend. Ook kan er dan een indicatie worden gemaakt van de verdere doorlooptijd van het plan. • De LMVW kan worden aangevuld met locaties die niet terugkomen in de plancapaciteit, zoals splitsingen van woningen. • De LMVW op planniveau kan worden aangevuld met CBS microdata via de IDs van verblijfsobjecten met een woonfunctie en de panden die daarbij horen. • Er zicht komt op woningbouwactiviteiten die niet geregistreerd staan in de planmonitors.
Epic.04/ US.02	BZK	Dat de technische oplossing aantallen woningen en behaalde mijlpalen toevoegt op basis van de in de BAG verkregen gegevens,	Er inzicht komt of woningen in het plan zijn vergund/de vergunning is ingetrokken, of woningen in aanbouw zijn, of woningen gerealiseerd zijn, of woningen gesloopt zijn.
Epic.04/ US.03	BZK	Dat de technische oplossing op basis van plangeometrie uit de provinciale aanlevering binnen en buiten plannen relevante publicaties uit de LVBB en hun metadata kan opslaan met behulp van de DSO API's. Belangrijk zijn de publicatietitel, publicatietekst, locatiegegevens, publicatiedatum, referenties,	Er inzicht verkregen wordt op behaalde mijlpalen in het planproces en bekendmakingen gebruikt kunnen worden om zich te krijgen op woningbouwactiviteiten die niet geregistreerd staan in de planmonitors van de provincie.
Epic.04/ US.04	BZK	Dat de technische oplossing door een plan behaalde mijlpalen registreert op basis van relevante publicaties uit de LVBB	Er zicht verkregen wordt op de volgende mijlpalen: • Anterieure overeenkomst, • Omgevingsplanwijziging aankondiging, ter inzage, vaststelling • Omgevingsvergunning aanvraag/verlening/weigeren/verlengen termijn (OPA/BOPA bouw, natura2000, flora en fauna)

			• Besluit voorgenomen gronduitgifte/verkoop • Besluiten na bezwaar of beroep.
Epic.04/ US.05	BZK	Dat de technische oplossing op basis van plangeometrie uit de provinciale aanlevering de percelen binnen plangebieden met behulp van de BRK registreert,	De LMVW op planniveau kan worden aangevuld met CBS-microdata via de percelen en publicaties in de LVBB beter gekoppeld kunnen worden aan een plan. Percelen worden regelmatig genoemd in de publicatietekst.
Epic.04/ US.06	BZK	Dat de technische oplossing doorlooptijden tussen de behaalde mijlpalen berekent volgens een nog uit te werken gegevensmodel,	Er inzicht komt in de doorlooptijden van plannen en plausibiliteitstoetsen op de doorlooptijd beter worden.
Epic.04/ US.07	BZK	Dat de technische oplossing behaalde mijlpalen en doorlooptijden gebruikt voor aanvullende plausibiliteitscontroles	Er versterking is van de datakwaliteitsanalyse en terugkoppeling aan de provincies en stuurgroep LMVW kan worden gegeven.

Tabel 8 User Story's bij Epic 04: Het bewerken van gegevens en data-analyse op de LMVW-database

2.5. Het ontvangen en verwerken van gegevens van het CBS

Met de in het vorige onderdeel verkregen gegevens uit de BAG en de BRK kunnen er via het CBS aanvullende gegevens voor het plan verzameld worden. Uiteindelijk zal de opdrachtnemer de aanvullende gegevens op planniveau of hoger aggregatieniveau moeten verwerken in de LMVW. Een deel van de nodige data is op gemeenteniveau reeds toegankelijk bij het CBS.

Bij deze Epic behorende user story's zijn:

ID	Als	Wil ik	Zodat
Epic.04/ US.08	BZK	CBS-statistieken van vergunde, in aanbouw zijnde, gerealiseerde en gesloopte woningen op gemeenteniveau verzamelen, inclusief gegevens over prijssegmenten, eigendom, type woning, type realisatie,	Ik op gemeente, woondeal, provincie en landelijkniveau statistieken kan maken over de daadwerkelijke realisatie.
Epic.04/ US.09	BZK	Op basis van verblijfsobject en pand IDs uit de BAG en percelen uit de BRK aanvullende CBS-microdata over aantallen per prijssegment, woningtype, (grond)eigendom, realisatie type binnen en buiten aangeleverde woningbouwplan geometrie van de provincies,	Er inzicht komt in de daadwerkelijke realisatie binnen plannen en wat er gerealiseerd wordt buiten de geregistreerde plannen om.
Epic.04/ US.10	BZK	Op basis van verblijfsobject en pand IDs uit de BAG en percelen uit de BRK aanvullende CBS-microdata per woningbouwplan, type woning, naar kenmerken als type huishoudens, leeftijden, inkomensgroepen,	Er inzicht komt in de bewoning van verschillende type woningen en of specifieke doelgroepen komen te wonen in volgens het beleid passende woning typen.

Tabel 9 User Story's bij Epic 04: Het ontvangen en verwerken van gegevens van het CBS t.b.v. de LMVW

2.6. Terugkoppeling en geautomatiseerde rapportages

Na verwerking van alle gegevens vindt er terugkoppeling vanuit de LMVW plaats richting de stuurgroep LMVW en de provincies over de datakwaliteit. Deze terugkoppeling wordt gedaan in de vorm van een dashboard en PDF. Daarnaast wordt ook om advies gevraagd voor de doorontwikkeling van het gegevensmodel en de gegevensuitwisseling.

Epic 5 – Het opstellen en delen van data kwaliteits- en verwerkingsrapportages:

ID	Als	Wil ik	Zodat
Epic.05	BZK	Van data kwaliteits- en verwerkingsrapportages kunnen opstellen en delen,	Ik vanuit de LMVW aan de stuurgroep kan terugkoppelen wat de datakwaliteit is van de door de provincies aangeleverde datasets.
Input van de User Story:		Resultaat van de User Story:	
Aangeleverde gegevens van provincies t.b.v. de LMVW.		Een rapport over de datakwaliteit en verwerking van de aangeleverde gegevens van de provincies.	
Betrokken voorzieningen:		LMVW.	

Tabel 10 Epic 05: De datakwaliteitsanalyse

ID	Als	Wil ik	Zodat
Epic.05/ US.01	BZK	Dat opdrachtnemer rapporteert met een dashboard en PDF over de datakwaliteit van de provinciale aanlevering en wijze van controle aan de stuurgroep LMVW,	De stuurgroep zicht krijgt op de datakwaliteit en hierop kan sturen.
Epic.05/ US.02	BZK	Opdrachtnemer rapporteert met een dashboard en PDF over de herkomst en metadata van de provinciale aanleveringen (softwaresystemen gemeente/provincie, extractiedatum) aan de stuurgroep LMVW,	De stuurgroep zicht krijgt op de dataketen.
Epic.05/ US.03	BZK	Opdrachtnemer rapporteert met een dashboard en PDF per bron/landelijke voorziening/CBS data de wijze van gegevensverzameling, interpretatie, verwerking ten behoeve van de LMVW aan de stuurgroep LMVW,	De stuurgroep zicht krijgt op de toegevoegde waarde van de landelijke voorzieningen.
Epic.05/ US.04	BZK	Opdrachtnemer adviseert en ondersteunt de stuurgroep LMVW bij de doorontwikkeling van de gegevensuitwisseling (dataprotocol) en het gegevensmodel (basisset) van de LMVW,	De stuurgroep geholpen wordt bij de doorontwikkeling van de LMVW.

2.7. Het ontsluiten van de LMVW gegevens

De opdrachtnemer ontsluit de gegevens van de LMVW op een door de opdrachtnemer te hosten website. De volgende zaken zullen via deze website gehost en ontsloten worden:

1. De vastgestelde documenten van de stuurgroep LMVW (dataprotocol, basisset);
 2. De LMVW datasets (provinciale aanlevering, gegevens landelijke voorzieningen, gegevens CBS);
 3. Een dashboard met relevante gegevens over de woningbouwopgave;
 4. Een interactieve kaart.
- Op het dashboard zijn alle gegevens geaggregeerd gepresenteerd vanaf gemeenteniveau.
 - Het gaat om gegevens uit de datasets, aanvullende statistieken van het CBS en gegevens over de woningbouwdoelstellingen en afspraken;
 - Dashboards kunnen weergegeven worden op gemeenteniveau, provincieniveau, woondealniveau en landelijk niveau;
 - Dashboard heeft filteropties;
 - Het dashboard heeft een exportfunctie naar PDF, CSV voor de gepresenteerde figuren en het gehele dashboard.
 - Een interactieve kaart op een webpagina met de openbare data op planniveau, gemeenteniveau, woondealniveau en provinciaal niveau;
 - Met mogelijkheden om meerdere kaartlagen te laten zien en toe te passen zoals verschillende basiskaartlagen;
 - Met de mogelijkheid om meerdere kaartlagen te laten zien en toe te passen zoals met kaarten over stikstof, geluidscontouren, netcongestie, grondgebruik etc. Welke kaartlagen zichtbaar kunnen zijn kan veranderen door veranderende beleidsopgaven;
 - Geeft ook percelen (BRK), verblijfsobjecten met woonfunctie, panden (BAG) weer;
 - Geeft op de kaart ook verwijzing naar bekendmakingen over woningbouwplannen (al dan niet gekoppeld aan een plan);
 - Het is wenselijk dat de kaart heeft opties heeft om o.a. zichtbaarheid en transparantie aan te passen naar wens van gebruiker.
 - De interactieve kaart heeft filteropties voor de data uit de datasets, zoals woningtypen, prijssegmenten, opleverjaren, behaalde mijlpalen en een zoekfunctie.
 - De datasets worden beschikbaar gesteld als een vertrouwelijke variant en een openbare variant.
 - Een datadownload van de openbare data achter een formulier;
 - Een datadownload van de alle data (incl. vertrouwelijk) na akkoord voorwaarden;
 - Een API van de openbare gegevens achter een formulier;
 - Een API van alle data (incl. vertrouwelijk) na akkoord voorwaarden.

Epic 7 – Het presenteren van de woningbouwplannen in de LMVW:

ID/tag	Als	Wil ik	Zodat
Epic.06	BZK	De geverifieerde set aan gegevens over woningbouwplannen in Nederland en de resultaten van de analyses met de gegevens uit andere Nederlandse bronnen in een overzichtelijke format presenteren in de Landelijke monitor voortgang woningbouw (LMVW),	• Alle woningbouwplannen landelijk in beeld zijn gebracht (in voorbereiding en uitvoering, inclusief locatie en kenmerken); • Er kan worden gevolgd of er voldoende plancapaciteit is om de bouwdoelen te halen; • Er kan worden gestuurd op de voortgang en uitvoering van de woondeals; • Plannen beleidsmatig kunnen worden bijgesteld of moeten worden herijkt.
Input van de User Story:		Resultaat van de User Story:	
• De geverifieerde set aan gegevens over woningbouwplannen in Nederland.		• Presentatie van de woningbouwplannen in Nederland in de LMVW.	

Rapporten op gemeentelijk-, provinciaal-, woningdeal- en nationaal niveau.
Betrokken voorzieningen: De database met woningbouwplannen in de LMVW.

Tabel 11 Epic 07: Het presenteren van de woningbouwplannen in de LMVW

Bij deze Epic behorende user story's zijn:

ID	Als	Wil ik	Zodat
Epic.06/ US.01	BZK	Dat Opdrachtnemer een website met interactieve kaart, dashboard, datasets en vastgestelde documenten host,	Gebruikers eenvoudig toegang hebben tot de gegevens uit de LMVW.
Epic.06/ US.02	BZK	Dat de website en functionaliteiten beschikbaar zijn via de browser (Safari, Chrome, Firefox, Edge) via PC, tablet en mobiel,	Gebruikers gemakkelijk toegang hebben tot de LMVW.
Epic.06/ US.03	BZK	Dat Opdrachtnemer het vastgestelde gegevensmodel (doorontwikkeling basisset) en dataprotocol van de LMVW beschikbaar stelt op een webpagina,	Dataleveranciers en gebruikers zicht hebben op wat er in de LMVW zit.
Epic.06/ US.04	BZK	Dat de datasets beschikbaar worden gesteld via een API met passende opties rond dataprotocol, vertrouwelijkheid en beveiliging,	Openbare data publiek toegankelijk is en onderzoekers (en het CBS) gebruik kunnen maken van de vertrouwelijke data.
Epic.06/ US.05	BZK	Dat de datasets beschikbaar worden gesteld via gegevens export (CSV, Excel, GeoJSON, Geopackage), met passende opties rond dataprotocol, vertrouwelijkheid en beveiliging,	Openbare data publiek toegankelijk is en onderzoekers (en het CBS) gebruik kunnen maken van de vertrouwelijke data.
Epic.06/ US.06	BZK	Een interactieve kaart van de openbare woningbouwplannen, met mogelijkheid voor kaartlagen, filtering van gegevens, toelichting data,	- De Tweede Kamer wordt geïnformeerd hoe het staat met de verschillende plannen waarmee de woningbouwopgave wordt gerealiseerd. - Het toegankelijk wordt gemaakt voor een breder publiek en onderzoekers wat er in de dataset te vinden is.
Epic.06/ US.07	BZK	Een dashboard met statistieken over woningbouwplannen, realisaties, doelen op gemeentenniveau, woondealniveau, provinciaal niveau en nationaalniveau welke exporteerbaar is als PDF,	Overheden en politiek een gemeenschappelijk beeld kunnen hebben van de voortgang op de woningbouwopgave.

Tabel 12 User Story's bij Epic 07: Het presenteren van de woningbouwplannen in de LMVW

In de onderstaande figuur is de presentatie van de gegevens in de Websites met LMVW en WOBI-monitor gevisualiseerd.



Figuur 6 Websites met LMVW



Figuur 7 Rapportages op basis van de datasets/dashboards



Figuur 8 Het beschikbaar stellen van Open Data

2.8. Het ontvangen en verwerken van WOBI-gegevens

Tot slot wordt de LMVW- vanuit de Wet open overheid (Woo) – hergebruikt voor de publicatie van WOBI-gegevens. Vooralsnog staan deze gegevens op zichzelf, hoewel de gegevens vanuit de LMVW en WOBI in de toekomst voor analyse doeleinden allicht op basis van polygonen toch gekoppeld gaan worden.

Epic 8 – Het beschikbaar stellen van Open Data over woningbouwplannen en van WOBI-gegevens:

ID/tag	Als	Wil ik	Zodat
Epic.08	BZK	Gegevens van WOBI kunnen ontvangen en verwerken op de LMVW website,	Deze gegevens in een aparte publieke WOBI-monitor op de LMVW website gepubliceerd kunnen worden.
Input van de User Story:		Resultaat van de User Story:	
De geverifieerde set aan gegevens over woningbouwplannen in Nederland.		Rapporten over de woningbouw in gemeenten, provincies en Nederland.	
Betrokken voorzieningen:		De database met woningbouwplannen en gerealiseerde woningen in gemeenten, provincies en Nederland.	

ID	Als	Wil ik	Zodat
Epic.08/ US.06	BZK	Gegevens van WOBI kunnen ontvangen en verwerken,	Deze gegevens in een aparte publieke WOBI-monitor op de LMVW website gepubliceerd kunnen worden.

Tabel 13 User Story's bij Epic 08: De van WOBI ontvangen gegevens publiceren in een WOBI-monitor

2.9. Het presenteren van de WOBI-gegevens

Het presenteren van de WOBI-gegevens in de WOBI-monitor voor publiek gebruik.

Epic 9 – Het presenteren van de WOBI-gegevens in de LMVW:

ID/tag	Als	Wil ik	Zodat
Epic.09	BZK	De WOBI-gegevens in een overzichtelijke format presenteren in de Landelijke monitor voortgang woningbouw (LMVW),	Deze gegevens publiekelijk beschikbaar zijn.
Input van de User Story:		Resultaat van de User Story:	
De set aan WOBI-gegevens.		Presentatie van de WOBI-gegevens op de LMVW website.	
Betrokken voorzieningen:		De database met woningbouwplannen en WOBI-gegevens op de LMVW website.	

Tabel 14 Epic 09: Het presenteren van de WOBI-gegevens in de LMVW

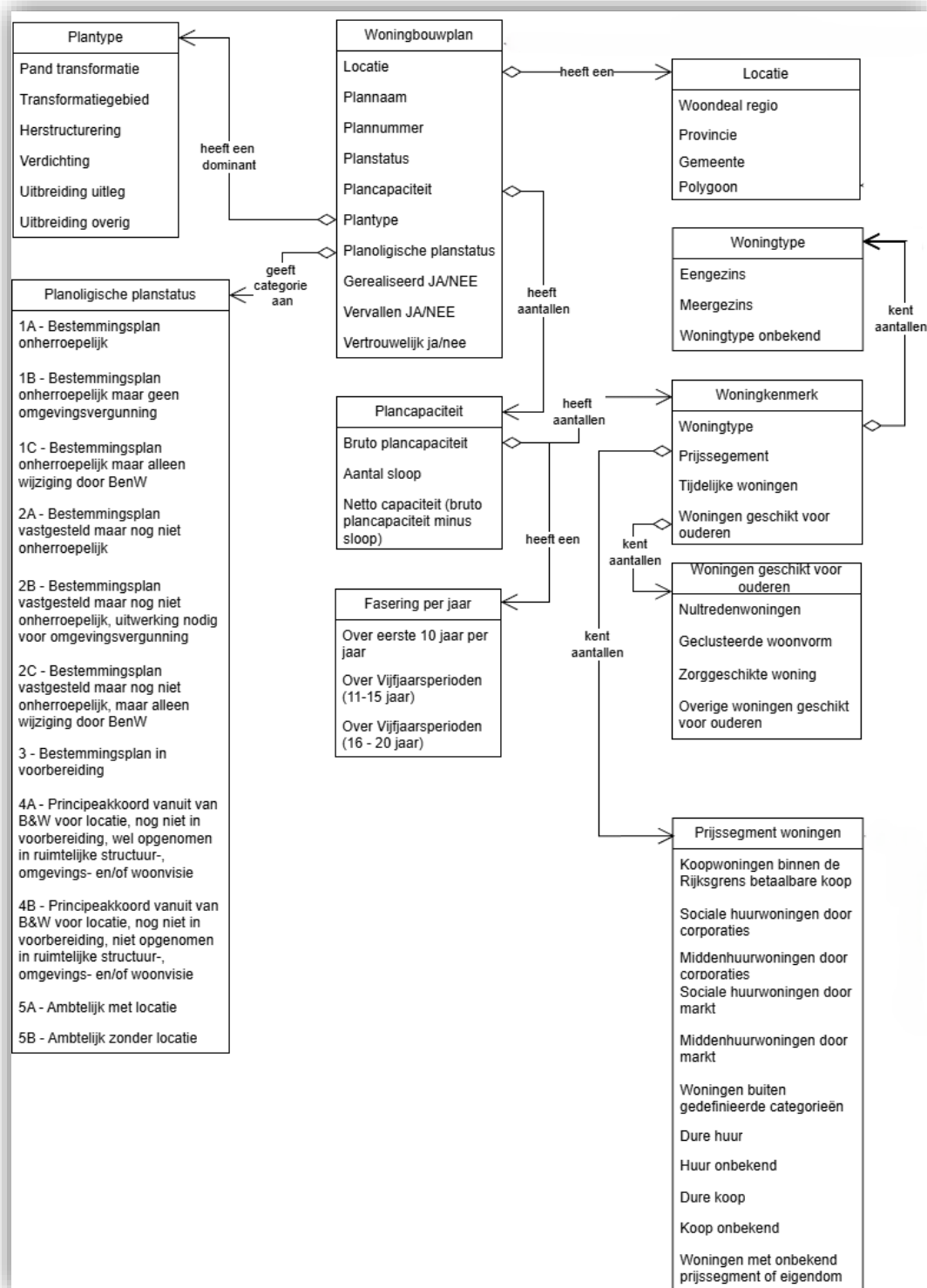
Bij deze Epic behorende user story's zijn:

ID	Als	Wil ik	Zodat
Epic.07/ US.01	BZK	Dat de WOBI-gegevens worden gepresenteerd in het WOBI- dashboard en de interactieve kaart op de LMVW website,	Deze gegevens publiekelijk beschikbaar zijn.

Tabel 15 User Story's bij Epic 09: Het presenteren van de WOBI-gegevens op de LMVW website

Bij de beschrijving van het proces wordt gesproken over gegevensuitwisselingen. Om welke gegevens het gaat en waar de uitwisselingen zitten wordt in dit hoofdstuk nader toegelicht.

In de onderstaande figuur zijn de uitgevraagde informatieattributen in een datamodel uitgewerkt.

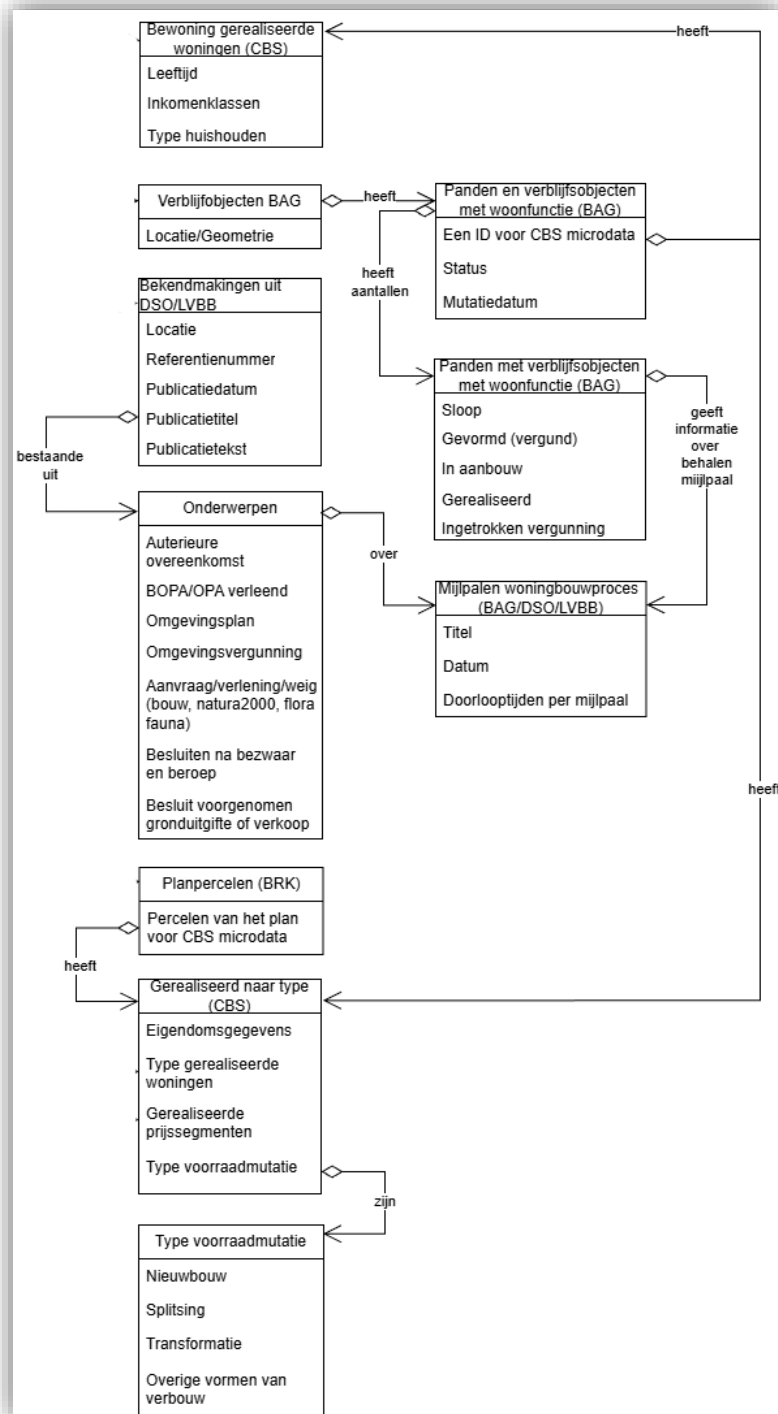


Figuur 9 Het datamodel van informatieattributen van de gemeentelijke/provinciale uitvraag in de LMVW

Voor de toelichting op, de semantiek van en de rationale van de gebruikte informatieattributen wordt verwezen naar het document “Basisset 2.0 Landelijke monitoring voortgang woningbouw (LMVW) vastgesteld in BO VRO mei/juni 2024”.

3.2. Het datamodel van aanvullende gegevens uit diverse bronnen

In de onderstaande figuur zijn de uitgevraagde informatieattributen in een datamodel uitgewerkt.



Figuur 10 Het datamodel van aanvullende informatieattributen uit Nederlandse bronnen in de LMVW

3.2.1. Uitvraag bij de BAG

De BAG is een landelijke voorziening die wordt beheerd door het Kadaster. Gemeenten zijn daarin de bronhouder, registratiehouder en verantwoordelijk voor de kwaliteit en actualiteit van het register. De wettelijk basis hiervoor is vastgelegd wet basisregistratie adressen en gebouwen (Wet BAG). Bestuursorganen mogen BAG-gegevens binnen hun publieke taak hergebruiken. Hiervoor is wel een autorisatiebesluit nodig, waarin wordt vastgelegd welke gegevens het bestuursorgaan (VRO) wil afnemen en voor welk doel ze die gegevens willen gebruiken (de rationale).

De gegevens die vanuit de LMVW bij het BAG worden uitgevraagd zijn:

- De IDs (bouwsteen voor CBS-microdata), planstatus en mutaties/updates (datum vergunning verleend, in aanbouw, volledig gerealiseerd) van het aantal verblijfsobjecten met een woonfunctie en de bijhorende panden binnen de geometrie van de plannen aangeleverd door de provincies. Dit attribuut heeft de LMVW nodig voor:
 - Het aantal woningen dat is gerealiseerd, vergund, in aanbouw, gesloopt binnen een plan;
 - De bereikte mijlpalen en doorlooptijden van het plan via de status van de verblijfsobjecten of de panden binnen het plan;
 - De verblijfsobject IDs en pand IDs voor gebruik van de CBS-microdata.
- De IDs (bouwsteen voor CBS-microdata), planstatus en mutaties/updates (datum vergunning verleend, in aanbouw, volledig gerealiseerd) van het aantal verblijfsobjecten met een woonfunctie en de bijhorende panden buiten de geometrie van de plannen aangeleverd door de provincies. Dit attribuut heeft de LMVW nodig voor:
 - Het aantal woningen dat is gerealiseerd, vergund, in aanbouw, gesloopt buiten de plannen om;
 - De verblijfsobject IDs en pand IDs om gebruik van de CBS-microdata mogelijk te maken.

3.2.2. Uitvraag bij het DSO/LVBB

Bij het Digitaal Stelsel Omgevingswet (DSO), de Landelijke Voorziening Bekendmaken en Beschikbaar stellen (LVBB) kent een wettelijke basis vanuit de Omgevingswet en registratiewetgeving. Het DSO is juridisch verankerd in:

- de Rijksoverheid Omgevingswet;
- het Omgevingsbesluit;
- de Regeling standaarden publicaties Omgevingswet;
- en onderliggende AMvB's en ministeriële regelingen.

Bestuursorganen zijn t.b.v. het DSO wettelijk verplicht om omgevingsdocumenten digitaal beschikbaar te stellen, standaarden te gebruiken en besluiten via de landelijke voorziening via een digitale uitvoering en technische normering te ontsluiten. Denk daarbij aan:

- hoe plannen gepubliceerd worden;
- metadata;
- geometrie;
- juridische regels.

De LVBB is de officiële publicatievoorziening binnen het DSO en heeft een wettelijke basis vanuit de Omgevingswet. Vanuit de LMVW worden de volgende attributen bevraagd:

- De publicatietitel, publicatietekst, datum, locatie en andere metadata van bekendmakingen binnen de geometrie van de door de provincies aangeleverde plannen. Dit attribuut heeft het LMVW nodig voor het achterhalen van bereikte mijlpalen in het woningbouwproces binnen de plangebieden zoals gekregen in de provinciale aanleveren. Het gaat om ten minste de volgende publicaties:
 - Anterieure overeenkomst afgesloten;
 - BOPA/OPA aangevraagd/verleend;
 - Omgevingsplan gewijzigd;

- Omgevingsvergunning aanvraag/verlening/weigeren (activiteiten bouwen, natura2000, flora en fauna);
 - Besluit voorgenomen gronduitgifte/verkoop;
 - Besluiten na bezwaar of beroep.
- Geldende regels omgevingsplan en mutaties daarvan binnen de geometrie van woningbouwplannen.

3.2.3. Uitvraag bij de BRK

De BRK is de Basisregistratie Kadaster, kent zijn wettelijke basis in de Kadasterwet, de Wet basisregistraties en het Burgerlijk Wetboek (registergoederen) en is een authentieke basisregistratie met verplichte afname en wettelijke terugmeldplicht. Dat betekent dat overheden de gegevens móéten gebruiken, tenzij er gerede twijfel bestaat. De BRK bevat zaken als:

- eigendom;
- zakelijke rechten;
- hypotheke;
- kadastrale percelen;
- tenaamstellingen.

Vanuit de LMVW worden alleen de kadastrale percelen bevraagd welke gerelateerd zijn aan de geometrie/locatie van de aangeleverde woningbouwdata door provincies. Dit attribuut heeft het LMVW nodig voor de het gebruik maken van de CBS microdata.

3.2.4. Uitvraag bij het CBS

Het CBS verzamelt gegevens die voor de LMVW relevant zijn. De grondslag hiervoor is vastgelegd in de Wet op het Centraal bureau voor de statistiek. Die wet geeft het CBS namelijk de bevoegdheden om:

- gegevens te verzamelen;
- registraties te koppelen;
- statistieken op te stellen;
- bestuursorganen om gegevens te verzoeken.

Op basis hiervan maakt het CBS gebruik van bestaande registraties, zodat ze gegevens niet zelf hoeft uit te vragen. Hiermee worden administratieve lasten gereduceerd. In dit kader gebruikt het CBS daarom gegevens vanuit de BAG. De gegevens die bij het CBS kunnen worden uitgevraagd zijn:

- Via de verblijfsobject IDs en pand IDs kan binnen woningbouwplannen kunnen de volgende kenmerken uit de microdata bij het CBS worden opgevraagd:
 - Prijssegmenten woningen binnen het plan en de prijsontwikkeling (blijven betaalbare woningen betaalbaar);
 - Woningtypen (meergezins-, eengezinswoningen) binnen het plan;
 - Eigendomssituatie binnen het plan (koop, huur);
 - Type realisatie (nieuwbouw, transformatie, splitsing) binnen het plan;
 - Realisatie (wordt daadwerkelijk gerealiseerd wat werd gepland in prijssegmenten en type woningen);
 - De mogelijkheid om analyse te doen naar de bewoning van het gerealiseerde plan. Denk aan: Leeftijd, type huishouden, inkomensgroepen in zoverre dit relevant is voor de monitoring of uitvoering van het woningbouwbeleid. Hierbij dient rekening gehouden te worden met persoonsgegevens in zowel verwerking als publicatie. Er kan eventueel gekozen worden om verwerking door het CBS uit te laten voeren.
- Via de verblijfsobject IDs en pand IDs buiten woningbouwplannen dezelfde gegevens ophalen, zoals hierboven beschreven over IDs binnen plannen.
- Via de percelen binnen woningbouwplannen gegevens ophalen voor woningbouwplannen, waar nog geen (nieuwe) verblijfsobjecten met woonfunctie zijn gevormd.

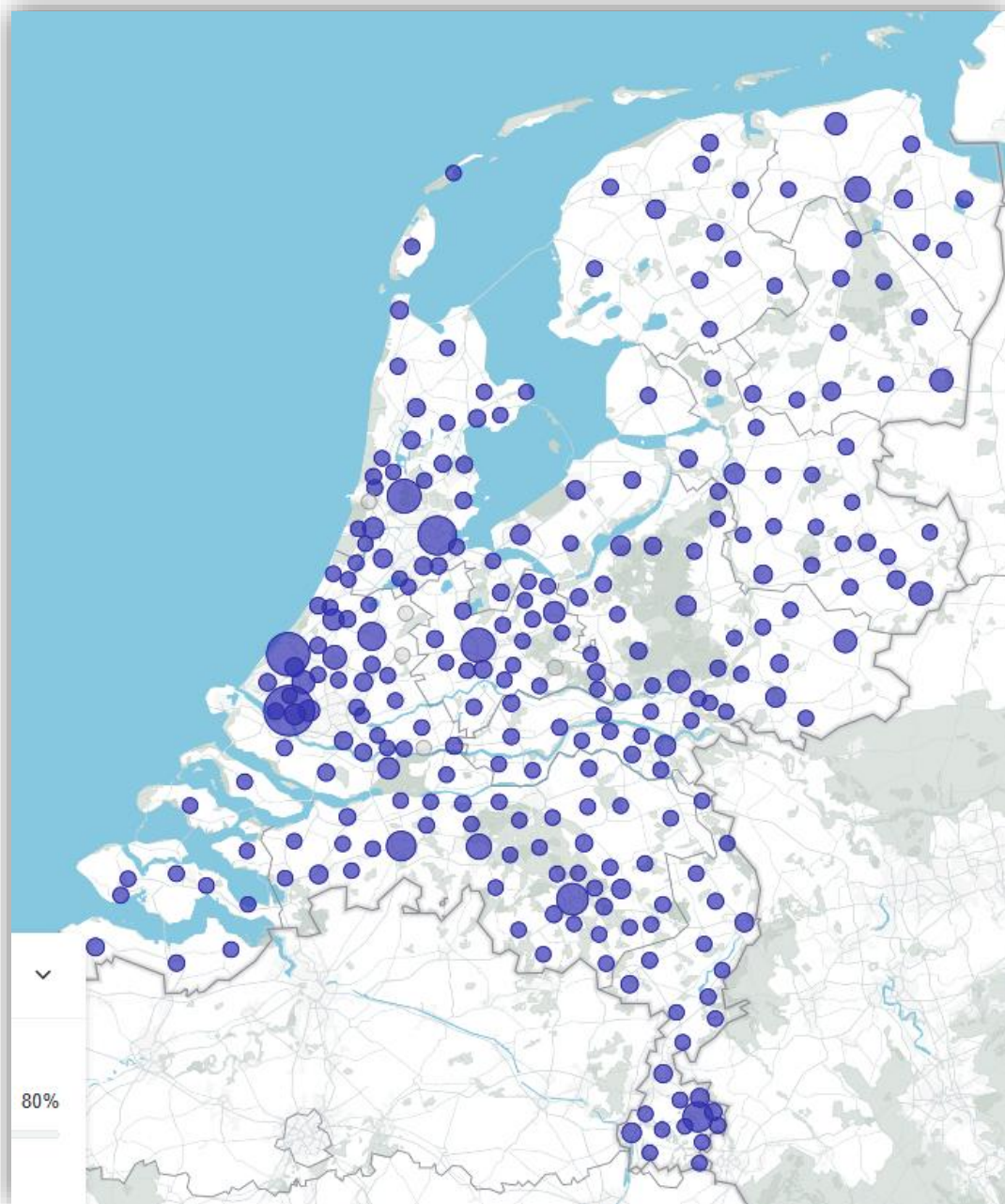
Volledigheidshalve is in de onderstaande figuur het gehele informatiemodel van de LMVW afgebeeld.



Het doel van het externe WOBI-dashboard is dat informatie van woningbouwprojecten met een Rijksbijdrage op een inzichtelijke wijze openbaar worden gemaakt t.b.v. de Woo. Dit is een aparte monitor die los staat van de LMVW-monitor en die binnen de LMVW-voorziening separaat moet worden ingericht. De LMVW-voorziening wordt daarmee een presentatie-platform van verschillende monitoren.

- het Woningbouwimpuls (WBI),
- de Startbouwimpuls (SBI),
- de Stimuleringsregeling Flex- en Transformatiewoningen (SFT),
- de Regeling Huisvesting Aandachtsgroepen (RHA),
- het Volkshuisvestingsfonds (VHF),
- en de Metropoolregio Eindhoven (WMRE).

Het dashboard wordt gepresenteerd als interactieve landkaart van Nederland. Deze landkaart geeft op gemeenteniveau de projecten weer. Hieronder een screenshot van het interne dashboard. Iets vergelijkbaars moet er ook komen voor de projectinformatie op het externe dashboard.



Figuur 12 Visualisatie van woningbouwprojecten met een financiële bijdrage vanuit het Rijk in een landkaart

Door op een gemeente (stip) te klikken verschijnt er een pop-up met detail informatie over de projecten die een financiële bijdrage hebben gekregen, als weergegeven in de volgende figuur (de naamgeving van de kolommen staat nog niet vast).

Projecten in Lan							X
Projectnaam	Regeling	Tranche	Woningen	Bijdrage	Start	Afronding	
LOO Noordpol	SFT	SFT2023	132	€ 1.029.600	25-03-2026	25-03-2027	
Sport	SFT	STIM2022	40	€ 1.584.000	30-06-2023	31-01-2024	

Figuur 13 Presentatie van detailinformatie in een gemeente

De gegevens worden aangeleverd door de RWB afdeling PMO. De verantwoordelijkheid voor de gegevens ligt bij RWB en kan op elk willekeurig moment in het dashboard worden verwerkt. In de praktijk zal dit 1x per maand zijn of gelijk lopen met de kwartaalrapportage. De gegevens worden handmatig geüpload en is vervolgens direct automatisch beschikbaar in het dashboard.

De volgende gegevens wordt in het dashboard publiekelijk gepresenteerd:

Data	Publiceren in extern dashboard?
Projectnaam	Ja (tekstveld)
Gemeente	Ja (tekstveld)
Provincie	Ja (tekstveld)
Regeling	Ja (tekstveld)
Tranche	Ja (tekstveld)
Totaal woningen	Ja (integer)
Financiële bijdrage	Ja (numeriek)
Datum start volgens beschikking	Ja (datum)
Datum afronding volgens beschikking	Ja (datum)

Figuur 14 De gepresenteerde WOBI-gegevens in het publieke WOBI-dashboard

4. Classificatie van gegevens en informatiebeveiliging

De grondslag voor het uitvragen van de geïntroduceerde gegevensverwerkingen t.b.v. LMVW, zijn vastgelegd in interbestuurlijke afspraken, convenanten en woondeal-afspraken tussen het ministerie van BZK, directie VRO, VNG, IPO en provincies en gemeenten. Deze hebben geresulteerd in standaardisaties van de uitvraag van gegevens (de Basisset 2.0).

In dit hoofdstuk zijn de gegevensbewerkingen onderzocht i.r.t. de risico's bij vertrouwelijkheid, integriteit en beschikbaarheid en het beveiligingsniveau dat nodig is om de geclassificeerde gegevens te beschermen.

4.1. Uitgevraagde gegevens via gemeenten/provincies

De via gemeenten en provincies uitgevraagde gegevens bevatten geen directe persoonsgegevens. Dit komt omdat het primair om projecten, locaties, aantallen woningen en plannings gaat. Maar zodra er met locaties wordt gewerkt, kan de locatie in sommige gevallen projectdata herleidbaar zijn naar een eigenaar of ontwikkelaar. In dat geval is de AVG (art. 6 lid 1 sub e⁴) van toepassing. Dit betekent: *"de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen"*. Voor het Rijk/provincies/gemeenten is woningbouwmonitoring namelijk onderdeel van publiek bestuur.

Een inbreuk op de vertrouwelijkheid, integriteit en beschikbaarheid van bovenstaande gegevens kan leiden tot risico's in juridische, bestuurlijke én praktische zin. Denk daarbij aan:

4.1.1. Schending van vertrouwelijkheid (ongoorloofde toegang of lekken)

De via gemeenten en provincies uitgevraagde gegevens bevatten geen directe persoonsgegevens. Wel kan het voorkomen dat locaties aan eigenaren of projectontwikkelaars zijn te koppelen. Echter, gezien de kans dat dit zich voordoet en de nadelige gevolgen die dit heeft wordt het als risico relatief laag ingeschat. Ook bevat de uitgevraagde gegevens informatie over de (mogelijk) prijsniveau van de individuele woningen binnen een woningbouwplan, hetgeen indirect iets zegt over de toekomstige bewoners. Gezien het feit dat deze informatie ook op andere openbare plekken beschikbaar is en de nadelige gevolgen die dit heeft beperkt zijn wordt het als risico relatief laag ingeschat.

Bepaalde gegevens hebben toch een vertrouwelijk karakter. Dit heeft vooral te maken met het voorbereiden van bouwplannen, welke nog niet met de samenleving zijn gedeeld. Het mag niet gebeuren dat burgers via de monitor te weten komen dat er bouwplannen zijn. Dit kan tot onrust leiden en ondermijnt het vertrouwen van burgers in de overheid. Dit is ook reden dat deze als vertrouwelijk gemarkeerde gegevens niet worden aangeleverd en dus ook niet in de LMVW worden opgenomen.

4.1.2. Schending van integriteit (onjuiste of gemanipuleerde gegevens)

Belangrijker is dat de integriteit van de gegevens goed wordt beveiligd. Wanneer de kwaliteit van de aangeleverde gegevens slecht is of wanneer onbevoegden gegevens in de LMVW-database kunnen wijzigen, dan dit leiden tot:

- Een onjuiste presentatie de werkelijkheid in de monitor en rapporten.
- Een verkeerd beeld van en verkeerde besluit- en beleidsvorming t.a.v. de woningmarkt.

Daarom zijn er maatregelen in termen van de bewaking van datakwaliteit en informatiebeveiliging noodzakelijk. Deze maatregelen zijn in de volgende paragraaf nader uitgewerkt.

4.1.3. Schending van beschikbaarheid (gegevens niet toegankelijk)

De LMVW wordt thans in principe slechts twee keer per jaar gerapporteerd, tenzij er eventueel tussentijdse updates via BAG/DSO zijn. Daarom wordt het risico t.a.v. de beschikbaarheid van de

⁴ [Artikel 6 - Rechtmatigheid van de verwerking | AVGb.nl](#)

gegevens momenteel als laag ingeschat. Dit zou in de toekomst kunnen veranderen wanneer de frequentie van rapportages toeneemt of zelfs realtime zou worden. Vooralsnog is daar nog geen sprake van.

4.2. Kaders voor informatiebeveiliging

Om bovenstaande risico's te mitigeren, zijn voor de Rijksoverheid geldende kaders op het gebied van informatiebeveiliging (zoals de Cyberbeveiligingswet (Cbw), BIO2 (VIR, VIR-BI), Rijkscloudbeleid, etc.) van toepassing voor verwerkers en hun leveranciersketen. In deze paragraaf zijn een aantal eisen vanuit de privacywetgeving en maatregelen vanuit de informatiebeveiliging opgesomd, ter bescherming van de gegevens.

Hoewel er via gemeenten en provincies gegevens worden uitgevraagd en verzameld, moeten er vooral vanuit de integriteit van de gegevens wel passende technische en organisatorische maatregelen worden genomen om de gegevens te beveiligen. Denk daarbij aan maatregelen in de sfeer van:

- Het vergroten van de datakwaliteit.
- Het voorkomen dat onbevoegden LMVW-gegevens kunnen wijzigen.

De minister van BZK is verantwoordelijk voor de integrale beveiliging en de inrichting en werking van de beveiligingsorganisatie. In die hoedanigheid is de minister van BZK ook eindverantwoordelijk voor de kwaliteit van de gegevens in de LMVW. Hieronder zijn de belangrijkste eisen in het kader van de bescherming van de gegevens samengevat.

4.2.1. Het vergroten van de datakwaliteit

De belangrijkste maatregelen voor het vergroten van de datakwaliteit:

- Bij de invoer van gegevens door gemeenten en provincies worden er t.a.v. de invoer controles uitgevoerd. Denk daarbij aan geautomatiseerde controles op volledigheid en geldigheid van data, zoals waar aantallen moeten worden ingevoerd mogen geen letters staan en visa versa, een begindatum mag nooit later zijn dan een einddatum, etc.
- Door gemeenten en provincies aangeleverde gegevens worden vergeleken en gecontroleerd a.d.h.v. gegevens aangeleverd door het CBS, de BAG, het DSO/LVBB en BRK.

ID	Als	Wil ik	Zodat
DK/ US.01	BZK	Dat de gegevens van de provincies op een uniforme en digitale wijze worden aangeleverd bij het LMVW,	De datakwaliteit en daarmee de integriteit van de gegevens t.b.v. het dashboard, rapportages en beleidsinformatie wordt versterkt en semantische verwarring, inconsistentie en administratieve lasten worden verlaagd.
DK/ US.02	BZK	Dat na automatische datacontroles onvolledigheid, ongeldigheid, inconsistentie, plausibiliteit op aangeleverde gegevens wordt signaleerd bij provincies en de eigenaar van het LMVW,	Er kan worden bijgestuurd wanneer de datakwaliteit niet aan de eisen voldoet en kan worden voorkomen dat er onjuiste data wordt gepresenteerd in de LMVW.
DK/ US.03	BZK	De van de provincies ontvangen gegevens kunnen analyseren en beoordelen op semantiek, datakwaliteit en uniformiteit,	Ik weet dat ik over een betrouwbare set van geverifieerde en gevalideerde gegevens beschik die ik kan presenteren in de LMVW.
DK/ US.04	BZK	Dat datakwaliteitsrapportages en samenvattende rapportages beschikbaar worden gesteld aan provincies en de stuurgroep LMVW,	Er kan worden bijgestuurd wanneer de datakwaliteit niet aan de eisen voldoet en kan worden voorkomen dat er onjuiste data wordt gepresenteerd in de LMVW.

Tabel 16 Eisen t.a.v. datakwaliteit

4.2.2. Het voorkomen dat onbevoegden LMVW-gegevens kunnen wijzigen

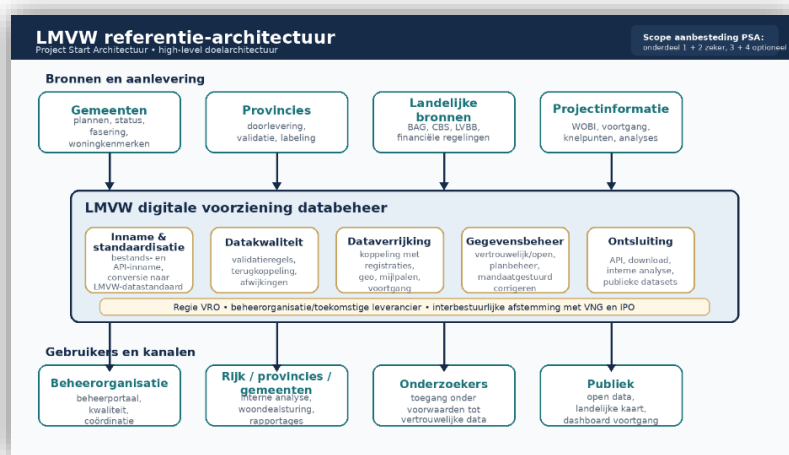
De belangrijkste maatregelen om te voorkomen dat onbevoegden LMVW-gegevens kunnen wijzigen:

- Gebruikers hebben vanuit hun taken alleen bevoegdheden voor zover dat voor de uitoefening van hun taak noodzakelijk is ("Need-to-know", "need-to-use"). Toegang tot informatie en systeemfuncties van toepassingen behoort daarom a.d.h.v. autorisatiebesluiten te worden beperkt tot die informatie die ze nodig hebben voor de uitoefening van hun taak en rol (Role-Based Access Control (RBAC)).
- Alle door de systemen uitgevoerde handelingen en handelingen van gebruikers, maar ook die van systeembeheerders en -operators in voorzieningen zijn vastgelegd in een volledige, eenduidige en herleidbare audittrail. Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
- De in LMVW vastgelegde gegevens worden end-to-end encrypted uitgewisseld en vastgelegd.
- In de ketens wordt er informatie uitgewisseld. Daarom worden er afspraken gemaakt over:
 - Het periodiek afleggen van een Statement of Compliance over de uitwisseling van informatie.
 - Het volgen van het standaard beveiligingsniveau dat hieraan worden gesteld.

ID	Als	Wil ik	Zodat
IB/ US.01	BZK	Dat de LMVW voldoet aan de eisen zoals die worden gesteld van uit de AVG en BIO2,	De LMVW voldoet aan het standaard beveiligingsniveau dat de Nederlandse overheid hieraan stelt.
IB/ US.02	BZK	Dat gebruikers alleen toegang hebben tot die functies en gegevens waarop ze vanuit hun rol ("Need-to-know", "need-to-use") toe bevoegd zijn,	Er geen ongewenst gebruik kan worden gemaakt van functies en gegevens in de LMVW.
IB/ US.03	BZK	Dat alle handelingen van gebruikers van het LMVW worden vastgelegd in een volledige, eenduidige en herleidbare audittrail en logbestanden,	Achteraf kan worden gereconstrueerd wat er in algemene zin – maar specifiek ook qua integriteit van de gegevens – is gebeurd.

Tabel 17 Eisen vanuit informatiebeveiliging

De volgende figuur laat de informatiestromen en de diensten in relatie tot de LMVW zien.



4.3. Afspraken over koppelvlakken voor het uitwisselen van informatie

Er zijn verschillende koppelvlakken voor informatie-uitwisseling tussen verschillende betrokken partijen benoemd. In dit hoofdstuk is beschreven volgens welke standaarden deze koppelingen in technische zin worden gerealiseerd.

In de informatie-uitwisselingen van de LMVW voort worden eisen gesteld aan de koppelingen bij het uitwisselen van informatie. Hierbij worden o.a. de standaarden van Nederlandse Forum voor Standaardisatie gevolgd.

Het Forum voor Standaardisatie positioneert Digikoppeling als de centrale koppelvlakstandaard voor veilige gegevensuitwisseling tussen overheden en GDI-voorzieningen. Het betreft dan ook een "Pas toe of leg uit" standaard (dus verplicht bij toepassing binnen de overheid). Het geldt vooral voor:

- koppelingen met basisregistraties,
- sector overstijgende uitwisseling en
- systemen met wederzijdse authenticatie en gecontroleerde uitwisseling.

Binnen de Digikoppeling verdient het REST API-profiel, gebaseerd op de landelijke REST API Design Rules, de voorkeur voor de uitwisseling van de gegevens tussen het LMVW en de gemeenten/provincies en de overige bronregisters. Daarbij is belangrijk dat:

Toegang

- Actoren mogen alleen vanuit hun specifieke rol en vanuit hun taak toegang (role bases access) verkrijgen tot de verwerking van de gegevens. Dit betekent dat het mogelijk moet zijn om een actor te kunnen identificeren, authenticeren en autoriseren.
- Voor digitale bevragingen van gegevens wordt bij de bevraging geautomatiseerd geïdentificeerd, geauthentiseerd en geautoriseerd. Deze controle maakt onderdeel uit van en is geïmplementeerd in de REST API van de Digikoppeling.
- Alle handelingen die toegang tot gegevens in de LMVW verschaffen en gebruikers die toegang hebben verkregen worden gemonitord en gelogd. Verder zijn al deze handelingen en personen achteraf traceerbaar in een audittrail.

Informatiebeveiliging

- Informatie-uitwisselingen tussen ketenpartijen moeten veilig worden afgehandeld en mogen tijdens de uitwisseling of presentatie niet worden onderschept. Mocht een bericht toch worden onderschept dan moet het door encryptie onmogelijk worden gemaakt om deze berichten te kunnen lezen.
- Er zijn bij informatie-uitwisselingen door zowel de verzendende – als door de ontvangende partij maatregelen genomen tegen virussen, malware, ransomware en andere soortgelijke bedreigingen.

Encryptie en End-to-End secure

Om te voorkomen dat gegevens worden gelezen door onbevoegden (inclusief beheerders), wordt gebruik gemaakt van encryptie tijdens zowel de vastlegging als tijdens de uitwisseling tussen actoren en applicaties.

Informatie-uitwisselingen tussen twee actoren verlopen daarom ook via end-to-end beveiligde verbindingen. API's kunnen zo worden ingericht, zodat ze hierin voorzien.

⁵ Project start architectuur (PSA) Landelijke Monitor Voortgang Woningbouw (LMVW), versie 0.1, maart 2026, Robin Vink

ID/tag	Als	Wil ik	Zodat
IB/ US.04	BZK	Dat de koppelingen voor gegevensuitwisseling voldoet aan de door Nederlandse Forum voor Standaardisatie voorgeschreven standaard Digikoppeling (de variant REST API),	Gegevens volgens de bij de Nederlandse overheid geldende standaard veilig worden uitgewisseld.
IB/ US.05	BZK	Dat alle gegevensaanleveringen aan het LMVW worden gecontroleerd op virussen, malware, ransomware en andere soortgelijke bedreigingen,	De LMVW en de gegevens niet worden besmet en de LMVW beschikbaar blijft voor gebruikers.
IB/ US.06	BZK	Dat alle gegevens: • end-to-end encrypted aan het LMVW worden aangeleverd, • encrypted in de LMVW worden vastgelegd en dat er centraal sleutelbeheer t.b.v. de encryptie plaatsvindt,	(On)bevoegden de uitgewisselde – of de vastgelegde gegevens van het LMVW niet rechtstreeks in de berichten of database kunnen zien of aanpassen.

Tabel 18 De non-functional requirements voor Overdraagbaarheid

5. Wet- en regelgeving vanuit de digitale overheid

In dit hoofdstuk zijn de (wettelijke) randvoorwaarden, voorschriften en kaders beschreven, welke van toepassing zijn op de informatievoorziening en welke randvoorwaarden van toepassing zijn vanuit de architectuur- en informatiebeveiliging.

5.1. De Baseline Informatiebeveiliging Overheid

Het BIO/kader van de Baseline Informatiebeveiliging Overheid 2 (BIO2⁶) is gestructureerd volgens NEN-EN-ISO/IEC 27001:2023, en deel 2 BIO-overheidsmaatregelen van de BIO2 is gestructureerd volgens NEN-EN-ISO/IEC 27002:2022. De BIO stelt de volgende verplichtingen aan entiteiten:

- **NEN-EN-ISO/IEC 27001 wordt toegepast op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging en het vaststellen van het toepassingsgebied van dit managementsysteem.** De BIO schrijft voor dat het managementsysteem van een entiteit voldoet aan NEN-EN-ISO/IEC 27001. Voor het bepalen van de context van de entiteit neemt de entiteit minimaal de bedrijfsprocessen en informatiesystemen op die kritisch zijn voor haar dienstverlening bij het inrichten, implementeren, in stand houden en continu verbeteren van het managementsysteem voor informatiebeveiliging.
- **NEN-EN-ISO/IEC 27002 en de verplichte overheidsmaatregelen uit de BIO worden toegepast op het formuleren van passende beheersmaatregelen.** Hierbij wordt rekening gehouden met de omgeving(en) waarin de informatiebeveiligingsrisico's gelden, gebaseerd op de scope en de onderkende risico's. De beheersmaatregelen uit NEN-EN-ISO/IEC 27002 en de BIO kunnen, waar nodig én gelijkwaardig worden vervangen of gecombineerd met beheersmaatregelen uit andere normen en richtlijnen, zoals voor zorginformatie NEN 7510 en voor Operationele Technologie (OT) de CSIR en IEC 62443 Industriële cybersecurity.
- **Entiteiten tonen opzet, bestaan en werking van maatregelen aan.** Dit vereiste volgt ook uit de Cbw/Network and Information Security directive 2 (NIS2).

Het Forum Standaardisatie heeft deze normen opgenomen in de 'pas toe-of-leg uit' lijst met verplichte standaarden voor de publieke sector in Nederland, volgens het 'comply or explain principe'. Dit betekent dat de overheid de voorgeschreven normen toepast, tenzij er expliciet geformuleerde redenen zijn om dat niet te doen. Een deel van de maatregelen is al weergegeven in de voorgaande paragraaf ("Kaders voor informatiebeveiliging").

5.2. Cyberbeveiligingswet (Cbw)

Voor overheden is in de Cbw vastgelegd op welke wijze de zorgplicht voor de beveiliging van netwerk- en informatiesystemen wordt ingevuld. Hieronder volgt een samenvatting van de belangrijkste punten die betrekking hebben op het toepassen van de BIO2:

- **Verplichting BIO2**
- Het toepassen van de BIO2 voor de beveiliging van netwerk- en informatiesystemen is via de Cbw verplicht voor alle entiteiten die vallen onder de sector 'Overheid'. Zie vorige paragraaf en hoofdstuk.
- **Verantwoordelijkheid bestuurder**
De bestuurder is verantwoordelijk voor:
 - het beheersen van informatiebeveiligingsrisico's en het treffen van passende en evenredige technische, operationele en organisatorische maatregelen om de risico's te beheren en afgestemd op de voor de entiteit relevante risico's en deze beheersen;
 - het goedkeuren van te nemen maatregelen voor het beheer van cyberbeveiligingsrisico's;
 - het toezien op de kwaliteit van de uitvoering en het beheer van de maatregelen.
- **Opleiding**

⁶ [Home NL - bio-overheid](#) , [ICO Wizard - bio-overheid](#)

Bestuurders zijn opgeleid en hebben kennis om te kunnen sturen op informatiebeveiligingsrisico's. Ze zorgen ervoor dat hun werknemers regelmatig opleiding/training volgen over het onderwerp. Dit betekent dat de opleiding voldoet aan de eisen uit de Cbw.

- **Meldplicht**
- De entiteit is verantwoordelijk voor het tijdig melden van significante incidenten. Overheden maken binnen de doorlooptijden een melding van een meldplichtig incident.
- **Toezicht en verantwoording**
- De toezichthouder zal toezicht houden op de invulling van de zorgplicht volgens de Cbw. De RDI is als toezichthouder aangewezen voor de sector 'Overheid'.

De bestuurder laat zich daarbij adviseren door een Chief Information Security Officer (CISO), Chief Information Officer (CIO), functionaris gegevensbescherming (FG) en dergelijke. Met name de CISO vervult hierin een belangrijk rol en:

- is verantwoordelijk voor de coördinatie van informatiebeveiliging;
- ondersteunt de bestuurder en geeft gevraagd en ongevraagd advies aan de bestuurder;
- vertaalt wetgeving en bedrijfsdoelstellingen naar een informatiebeveiligingsbeleid;
- rapporteert aan het bestuur hoe het lijnmanagement het informatiebeveiligingsbeleid implementeert en op welke wijze wordt voldaan aan de BIO, om ervoor zorg te dragen dat de bestuurder geïnformeerde besluiten kan maken over de behandeling van informatiebeveiligingsrisico's;
- is uitdrukkelijk niet verantwoordelijk voor informatiebeveiliging door het lijnmanagement.

5.3. Wet open overheid (Woo)

De Wet open overheid⁷ (Woo) is op 1 mei 2022 in Nederland in werking getreden en regelt het recht op informatie over alles wat de overheid doet. De Woo is bedoeld om overheden transparanter te maken, maar er zijn wel uitzonderingen. Zo moet de wet er in ieder geval voor zorgen dat overheidsinformatie beter vindbaar, uitwisselbaar, eenvoudig te ontsluiten en goed te archiveren is. Het grote verschil tussen de huidige Woo en de voorloper de Wob betreft de actieve openbaarmaking van overheidsinformatie. Dit betekent dat – naast de al passieve openbaarmaking n.a.v. een verzoek – men moet nadenken welke informatie allicht in aanmerking komt voor actieve openbaarmaking. Dit om de transparantie te bevorderen.

De LMVW draagt in een belangrijke mate bij aan transparantie over het behalen van doelen t.a.v. de woningbouw. Daarnaast wordt de overheid ook meer open en transparant wanneer de LMVW-gegevens als open data beschikbaar worden gesteld aan de samenleving.

ID	Als	Wil ik	Zodat
WG/ US.01	BZK	Dat de gegevens in de LMVW als open data beschikbaar worden gesteld aan derden,	Afnemers deze gegevens kunnen gebruiken voor eigen doeleinden.

Tabel 19 Eisen vanuit de wet open overheid

5.4. European Accessibility Act, EAA (Europese Toegankelijkheidswet)

Op 28 juni 2025 is de Europese Toegankelijkheidswet (European Accessibility Act, EAA⁸) ingegaan. Deze nieuwe wet is een grote stap in het toegankelijk maken van digitale producten en diensten voor mensen met een beperking. Aanbieders van digitale diensten in Nederland/Europa zijn wettelijk verplicht om hun diensten toegankelijk te maken voor iedereen. Daardoor is de invoering van de EAA digitale toegankelijkheid geen vrijblijvende ambitie meer, maar verplicht. Concreet houdt dit het volgende in:

⁷ [wetten.nl - Regeling - Wet open overheid - BWBR0045754](https://wetten.nl/Regeling-Wet%20open%20overheid-BWBR0045754)

⁸ [Nieuwe Europese toegankelijkheidswet - Digitale Overheid](#)

- Digitale producten moeten voldoen aan de toegankelijkheidsnormen⁹ (als [WCAG 2.1](#)).
- Toegankelijkheid moet vanaf de ontwerpfase (by design) meegenomen worden.
- Bestaande systemen moeten worden aangepast aan de nieuwe eisen. Soms is er een overgangperiode.
- Bedrijven krijgen boetes als ze niet aan de verplichtingen voldoen.

Overheidswebsites en apps in Nederland vallen al sinds 2018 onder het [Besluit digitale toegankelijkheid overheid](#)¹⁰. Voor overheden betekent dit dat die verplichtingen ongewijzigd blijven met de invoering van de EAA. Verder versterkt de nieuwe wet de aandacht voor digitale inclusie in beleid, ICT en dienstverlening. Dit betekent dat de website – die de gegevens van de monitor presenteert – moet voldoen aan de richtlijnen voor mensen met een beperking. Deze eis is als user story nader uitgewerkt bij bruikbaarheid in de niet functionele eisen.

5.5. Archiefwetgeving

De archiefwet 1995^{11,12} beschrijft regels en richtlijnen voor het archiveren van informatie door overheidsinstellingen. De Archiefwet is de belangrijkste wet voor de informatievoorziening van de Nederlandse overheid. De wet regelt dat overheidsarchieven na verloop van tijd openbaar worden voor burgers. De wet slaat op overheidsinformatie vanaf het moment dat die informatie wordt gemaakt. De belangrijkste bepaling van de wet is dat overheden hun informatie in goede, geordende en toegankelijke staat moeten brengen en bewaren. De informatie moet dus makkelijk te vinden en te raadplegen zijn. Ook moeten overheden zorgen voor de juridische overdracht van gegevens uit de LMVW naar het Nationaal Archief of voor de vernietiging van informatie die daarvoor in aanmerking komt.

Op 1 juli 2026 is de nieuwe archiefwet¹³ in werking is getreden, waarin diverse aanscherpingen zijn doorgevoerd. De archiefwet zelf is ook van toepassing op de LMVW. Dit geldt voor de gegevens in de LMVW, maar geldt ook voor de output (de presentatie van data op de website) en rapporten die eruit voortkomen wel.

5.6. De AI act

De AI-verordening is een Europese wet die regels stelt voor de ontwikkeling en het gebruik van AI-systemen en voor autonoom handelende computersystemen en algoritmes die beslissingen nemen, content genereren of mensen assisteren. Ook geeft de wet rechten aan burgers die in aanraking komen met AI-systemen. Het doel van de wet is dat AI-systemen die organisaties (binnen de EU) gebruiken, veilig zijn en fundamentele rechten respecteren en dat mensen en organisaties in de EU kunnen rekenen op veilige, transparante, traceerbare, niet-discriminerende en milieuvriendelijke AI-systemen onder menselijk toezicht. Het maakt daarbij niet uit of die AI-systemen binnen of buiten de EU zijn ontwikkeld. Dit speelt vooral een rol bij de selectie van uit te voeren inspecties d.m.v. algoritmen in het kader van risico-gestuurd toezicht.

In het kader van de LMVW worden geen algoritmen gebruikt die beslissingen nemen over burgers en is daarom niet van toepassing.

5.7. Het Nederlandse data-ecosysteem

De belangrijkste principes vanuit het Nederlandse data-ecosysteem zijn vastgelegd in het Federatief Datastelsel, de Nationale Datastrategie en de Interbestuurlijke Datastrategie.

⁹ [Richtlijnen voor Toegankelijkheid van Webcontent \(WCAG\) 2.1](#)

¹⁰ [Wat is verplicht? | Digitoegankelijk](#)

¹¹ [Wet- en regelgeving | Nationaal Archief](#)

¹² *Er is nieuwe archiefwetgeving in de maak. Dit kan implicaties hebben voor wat hier is beschreven. Zie de link: [Intrekking van de Archiefwet 1995 en vervanging door een nieuwe Archiefwet \(Archiefwet 20..\) | Tweede Kamer der Staten-Generaal](#)*

¹³ [De nieuwe Archiefwet: Wat gaat er veranderen?](#)

5.7.1. Federatief Datastelsel

Het centrale principe in het Federatief Datastelsel is dat gegevens worden afgenomen van de bronhouder. Het is daarom belangrijk dat de LMVW uitgaat van het ontsluiten, combineren en gebruiken van data uit de verschillende systemen van gemeenten, provincies en de aanvullende gegevensbronhouders, zoals de BAG, het DSO/LVBB, de BRK en het CBS. Belangrijke Eisen vanuit het Federatief Datastelsel zijn daarom het:

- Scheiden van databronnen, datadiensten en gebruikersfunctionaliteit.
- Ondersteunen van virtuele data-integratie en federatieve query's.
- Minimaliseren van kopieën van brondata.
- Vastleggen welke gegevens tijdelijk worden gerepliceerd en waarom.
- Zorgen voor bronverwijzingen en de herleidbaarheid er naar.

5.7.2. Nationale Datastrategie

De Nederlandse datastrategie richt zich op het verantwoord delen en hergebruiken van data. De LMVW kent geen eigen brongegevens en hergebruikt alleen gegevens die worden aangeleverd door gemeenten, provincies en de aanvullende gegevensbronhouders (de BAG, het DSO/LVBB, de BRK en het CBS). Dit vertaalt zich naar de volgende concrete eisen:

- *Data als strategisch bezit:* definieer eigenaarschap, beheer en kwaliteitsverantwoordelijkheid.
- *Eenmalige uitvraag, meervoudig gebruik:* hergebruik bestaande registraties en voorkom dubbele aanleveringen.
- *Open standaarden:* vermijd leveranciersafhankelijkheid.
- *Interoperabiliteit:* gebruik gestandaardiseerde definities, berichten en API's.
- *Privacy en ethiek by design:* voer een DPIA uit en implementeer passende waarborgen.
- *Transparantie:* maak inzichtelijk welke data waarvoor wordt gebruikt.

5.7.3. Interbestuurlijke Datastrategie

De interbestuurlijke datastrategie benadrukt dat er interbestuurlijk afspraken worden gemaakt over data. In het geval van LMVW betreft dit BZK, de provincies, de gemeenten en de aanvullende gegevensbronhouders (de BAG, het DSO/LVBB, de BRK en het CBS). Daarom is het vanuit de invalhoek van de Interbestuurlijke Datastrategie belangrijk de volgende aspecten in de Governance op te nemen:

- Beschrijf heldere rollen en verantwoordelijkheden voor bronhouders, afnemers en beheerders.
- Beschrijf de gemeenschappelijke semantiek en definities van de gegevens.
- Maak procesafspraken voor wijzigingsbeheer.
- Leg de afspraken en beschikbaarheid vast in servicelevels.
- Beschrijf de Governance voor datakwaliteit en incidentafhandeling.

6. Niet functionele eisen aan voorzieningen

In dit hoofdstuk zijn niet-functionele eisen opgesteld, waaraan de dienstverlening van de voorzieningen van de EU-richtlijn moeten voldoen. Voor het opstellen van de eisen is de ISO-norm 25010¹⁴ voor productkwaliteit gebruikt.

6.1. Functionele geschiktheid (Product Quality)

ID/tag	Als	Wil ik	Zodat
NF/ US.01	Afnemer van de LMVW	Dat de LMVW diensten levert die in effecten resulteert die in de functionele user story's zijn beschreven,	Ik mijn taken kan uitvoeren.

Tabel 20 De non-functional requirements voor Functionele geschiktheid

6.2. Prestatie-efficiëntie (Performance efficiency)

ID/tag	Als	Wil ik	Zodat
NF/ US.02	Afnemer van de LMVW	Dat handelingen in de LMVW zonder dat er een merkbare vertraging direct worden verwerkt,	Ik zonder oponthoud mijn werk kan doen.
NF/ US.03	Afnemer van de LMVW	Dat de LMVW bewerkingen van aanleverende – en afnemende partijen probleemloos en zonder prestatieverlies aan kan, ook wanneer er in de toekomst het aantal informatie-uitwisselingen of gegevenssets toeneemt,	De kwaliteit van dienstverlening in de LMVW intact blijft.

Tabel 21 De non-functional requirements voor Prestatie-efficiëntie

6.3. Uitwisselbaarheid (Compatibility)

ID/tag	Als	Wil ik	Zodat
NF/ US.04	Afnemer van de LMVW	Dat er in de ketens van de EU-richtlijn op de koppelvlakken van informatie-uitwisseling tussen de LMVW en aanleverende – en afnemende partijen afspraken zijn gemaakt over het gebruik van Interoperabele standaarden,	Informatie onderling probleemloos kan worden uitgewisseld.
NF/ US.05	Afnemer van de LMVW	Dat de gehanteerde standaarden in de voorzieningen en ketens van informatie-uitwisseling tussen de LMVW en aanleverende – en afnemende partijen voldoen aan voorgeschreven standaarden van het Nederlandse Forum voor Standaardisatie ¹⁵ ,	Informatie onderling probleemloos kan worden uitgewisseld.

Tabel 22 De non-functional requirements voor Uitwisselbaarheid

¹⁴ [ISO 25010 - Wikipedia](#)

¹⁵ [Lijst open standaarden](#) | [Forum Standaardisatie](#) en [Rijksregister standaarden - RORA Online](#)

6.4. Bruikbaarheid (Usability)

ID/tag	Als	Wil ik	Zodat
NF/ US.06	Afnemer van de LMVW	Dat er intuïtieve en toegankelijke gebruikersinterfaces voor de diensten zijn,	Mensen het systeem intuïtief en eventueel m.b.v. helpfuncties, etc. kunnen gebruiken en een gebruikersvriendelijke omgeving ervaren.
NF/ US.07	Eigenaar van de LMVW	Het LMVW voldoet aan de Europese Toegankelijkheidswet (European Accessibility Act, EAA16), wat betekent dat: - Digitale producten moeten voldoen aan de toegankelijkheidsnormen¹⁷ (als WCAG 2.1). - Toegankelijkheid moet vanaf de ontwerpfase meegenomen worden.	Ook mensen met een beperking het LMVW kunnen gebruiken, dat BZK aan wetgeving voldoet en wordt voorkomen dat BZK boetes krijgt als ze niet aan de verplichtingen voldoet.
NF/ US.08	BZK	Dat het dashboard en de interactieve kaart van de LMVW via de browser op ieder moment en via ieder device beschikbaar zijn,	Gebruikers eenvoudig toegang hebben tot de gegevens uit de LMVW.

Tabel 23 De non-functional requirements voor Bruikbaarheid

6.5. Betrouwbaarheid (Reliability)

ID/tag	Als	Wil ik	Zodat
NF/ US.09	Afnemer van de LMVW	Dat: - de LMVW op jaarbasis voor 99,5% beschikbaar is., - Gepplande momenten voor systeemonderhoud vallen buiten deze beschikbaarheidseisen,	De diensten van de LMVW praktisch altijd beschikbaar en toegankelijk zijn.
NF/ US.10	Afnemer van de LMVW	Dat: - de beschikbaarheidseisen van de LMVW zijn vastgelegd in een contract (SLA), - hierover wordt gerapporteerd en - er op de resultaten vanuit een beschreven governance actief wordt gestuurd,	- Prestaties meetbaar worden (inzicht), - Transparant is (overzicht) in hoeverre gemaakte afspraken worden gehaald en wie verantwoordelijk is voor het behalen ervan en - Wat er door wie aan gedaan wordt (sturen) wanneer dit niet het geval is.
NF/ US.11	Afnemer van de LMVW	Dat de LMVW foutmeldingen genereert wanneer er fouten optreden en dat deze foutmeldingen worden verzameld,	A.d.h.v. veel voorkomende foutmeldingen Opdrachtnemer onderhoudswerkzaamheden kan initiëren of plannen.
NF/ US.12	Afnemer van de LMVW	Dat bij verstoringen of uitval van de LMVW al uitgevoerde bewerkingen worden bewaard en hersteld na het uitvallen of	De consistentie van het systeem is gewaarborgd.

¹⁶ [Nieuwe Europese toegankelijkheidswet - Digitale Overheid](#)

¹⁷ [Richtlijnen voor Toegankelijkheid van Webcontent \(WCAG\) 2.1](#)

het tijdelijk niet beschikbaar zijn
van de LMVW,

Tabel 24 De non-functional requirements voor Betrouwbaarheid

6.6. Beveiligbaarheid (Security)

ID/tag	Als	Wil ik	Zodat
NF/ US.13	Burger	Dat de in de LMVW vastgelegde gegevens zijn de geclassificeerd en a.d.h.v. gestelde eisen van informatiebeveiliging zijn beschermd,	Dat de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens zijn gewaarborgd en dat er geen onbevoegd – of misbruik van mijn en in het bijzonder van mijn privacygevoelige gegevens wordt gemaakt. Dit is in hoofdstuk 4 nader uitgewerkt.

Tabel 25 De non-functional requirements voor beveiligbaarheid

6.7. Onderhoudbaarheid (Maintainability)

ID/tag	Als	Wil ik	Zodat
NF/ US.14	Beheerder van de LMVW	Dat de LMVW flexibel is ingericht,	Er in de toekomst meer databronnen snel kunnen worden aangesloten, zonder dat daarvoor veel inspanningen of grote aanpassingen voor nodig zijn.
NF/ US.15	Beheerder van de LMVW	De impact, complexiteit en effecten van een wijziging kunnen bepalen,	Ik kan inschatten of een wijziging qua impact gewenst is en om te kunnen bepalen of en wanneer deze moet worden doorgevoerd.
NF/ US.16	Beheerder van de LMVW	Dat alle functionele – en niet functionele wijzigingen die op het systeem worden doorgevoerd, voor, tijdens en na de realisatie van de wijziging worden gelogd en via een onwijzigbare systeemlogging kunnen worden aangetoond,	Ik achteraf kan reproduceren en analyseren wat er is gebeurd.
NF/ US.17	Beheerder van de LMVW	Dat er afspraken worden gemaakt, afgestemd, gecommuniceerd en bewaakt over een service window dat voor alle aanleverende – en afnemende ketenpartijen periodiek geldt,	Bij alle partijen bekend is wanneer onderhoudswerkzaamheden worden uitgevoerd die geen effect hebben op de beschikbaarheid de LMVW.

Tabel 26 De non-functional requirements voor Onderhoudbaarheid

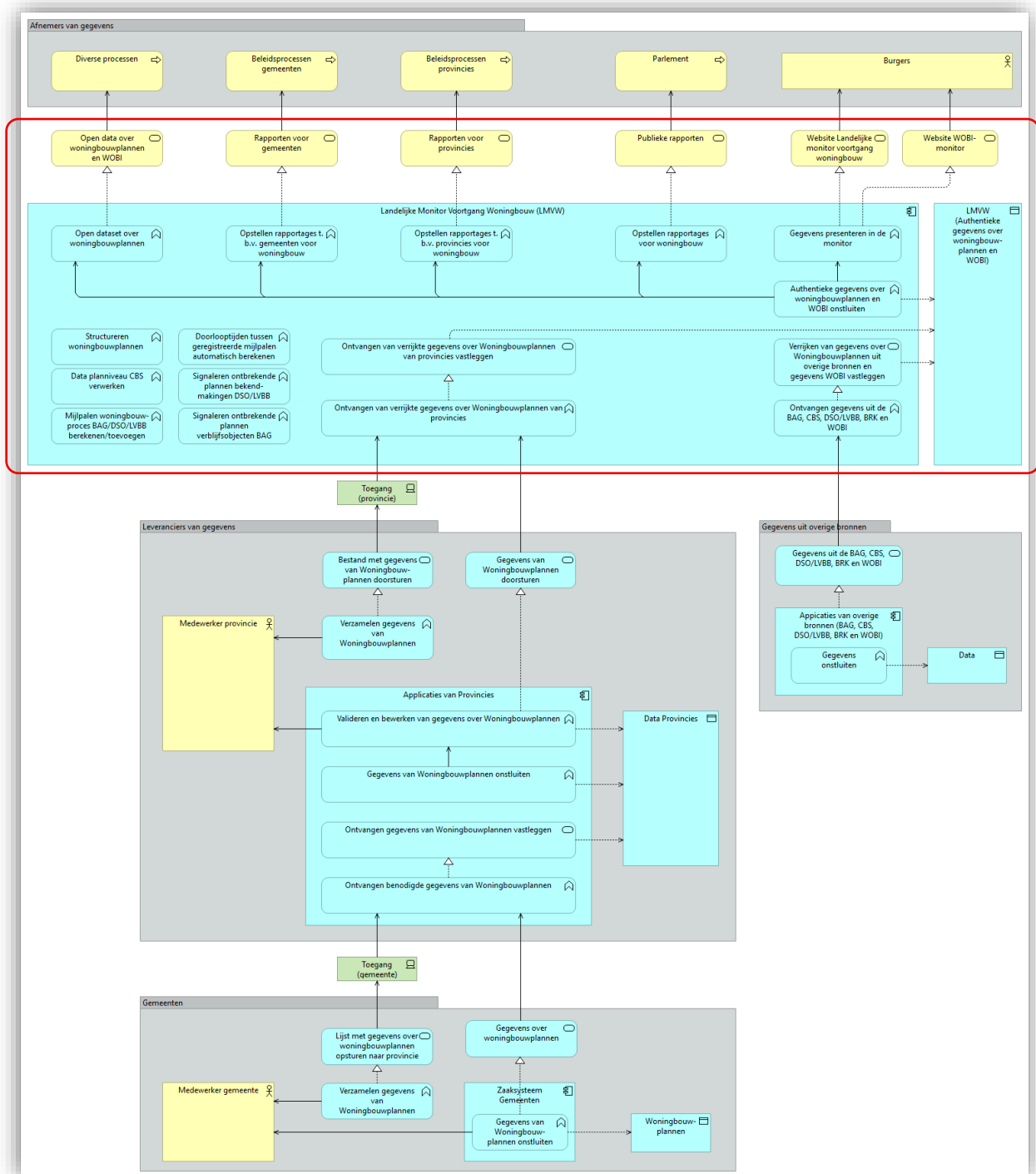
6.8. Overdraagbaarheid (Portability)

ID/tag	Als	Wil ik	Zodat
NF/ US.18	Beheerder van de LMVW	Dat de LMVW gemakkelijk bij een willekeurige hosting partij kan worden ondergebracht,	Ik niet afhankelijk ben van de hosting partij.
NF/ US.19	Beheerder van de LMVW	Dat de in de LMVW vastgelegde gegevens en applicatie zijn ontkoppeld,	De gegevens eenvoudig zijn over te brengen of om te zetten (dataportabiliteit) naar een nieuwe omgeving of informatievoorziening en ik niet afhankelijk ben van de leverancier van de applicatie.

Tabel 27 De non-functional requirements voor Overdraagbaarheid

7. Applicatielandschap

In de onderstaande figuur zijn in turquoise de applicaties benoemd die een rol spelen in de LMVW. Het deel dat in het rode blok is gemarkeerd betreft de LMVW en de diensten die de LMVW levert. Daaronder zijn aan de linkerkant de applicaties van de keten vanaf de gemeenten naar de provincies en de LMVW weergegeven.

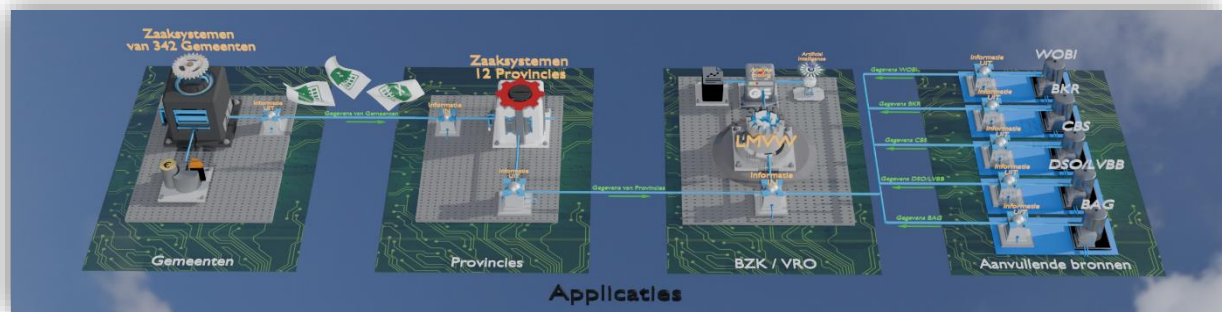


Figuur 16 Overzichtsplaat met functies en uitwisselingen

Dit betreft de leveringen van de woningbouwplannen. Aan de rechterkant zijn de gegevensleveringen van de overige aanvullende gegevensbronnen inclusief de WOBI ingetekend. Tussen de gemeenten en provincies, maar ook tussen de provincies en de LMVW is in het groene blokje nog "toegang" benoemd. Dit betreft de handmatige upload van bestanden. Bij de upload van

de WOBI-gegevens zou een vergelijkbare wijze van toegang moeten worden geregeld. In het geval van een digitale uitwisseling van de gegevens is de toegang in de REST API's geregeld.

In de onderstaande figuur is het applicatielandschap en de koppelingen in een visualisatie weergegeven.



Figuur 17 Visuele weergave van het applicatielandschap

8. Eisen vanuit de BIO2 t.a.v. de gebruikte gegevens

De Baseline Informatiebeveiliging Overheid (BIO2) is geheel gestructureerd volgens NEN-ISO/IEC 27001:2017, bijlage A en NEN-ISO/IEC 27002:2017. Het Forum Standaardisatie heeft deze normen opgenomen in de 'pas toe-of-leg uit'- lijst met verplichte standaarden voor de publieke sector, volgens het 'comply or explain principe'. Dit betekent dat de overheid deze normen toepast, tenzij er expliciet geformuleerde redenen zijn om dat niet te doen.

De meest essentiële maatregelen uit de BIO behorend bij BBN2 zijn hieronder opgesomd.

Informatiebeveiligingsbeleid	
5.1.1	Ten behoeve van informatiebeveiliging is er een reeks beleidsregels gedefinieerd, goedgekeurd, gepubliceerd en gecommuniceerd aan medewerkers en alle relevante betrokken partijen. Nice-to-have is wanneer de aanvullende eisen vanuit de NIS2 hierin zijn verwerkt.

Tabel 28 Eisen uit de BIO t.a.v. informatiebeveiligingsbeleid

Organiseren van informatiebeveiliging	
6.1.1	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd, gebaseerd op relevante voorschriften en wetten. Er is binnen de RCN een CISO aangesteld die conform dat vastgestelde CISO-functieprofiel toezicht houdt op de informatiebeveiliging.

Tabel 29 Eisen uit de BIO t.a.v. organiseren van informatiebeveiliging

Informatieclassificatie	
8.2.1	De informatie in voorzieningen zijn d.m.v. een expliciete risicoafweging geclassificeerd, zodat duidelijk is welk beschermingsniveau nodig is.

Tabel 30 Eisen uit de BIO t.a.v. Informatieclassificatie

Toegangsbeveiliging	
9.1.1	Er is beleid opgesteld voor toegangsbeveiliging, welke is vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.
9.1.2	Alleen geauthentiseerde gebruikers en apparatuur behoort toegang te krijgen tot functies, het netwerk en de netwerkdiensten, waarvoor zij specifiek bevoegd zijn.
9.4.1	Toegang tot gegevens en systeemfuncties van toepassingen behoren te worden beperkt tot die gegevens die nodig zijn voor de uitoefening van hun taak.
9.4.4	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, behoort te worden beperkt en nauwkeurig te worden gecontroleerd.
9.4.5	Toegang tot de programmabroncode is beperkt.

Tabel 31 Eisen uit de BIO t.a.v. toegangsbeveiliging

Cryptografie	
10.1.1	Ter bescherming van gegevens behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd. Denk aan cryptografiebeleid, waarin minimaal de volgende onderwerpen zijn uitgewerkt: a) Wanneer cryptografie ingezet wordt. b) Wie verantwoordelijk is voor de implementatie. c) Wie verantwoordelijk is voor het sleutelbeheer. d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. e) De wijze waarop het beschermingsniveau vastgesteld wordt. f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.
10.1.2	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.

Tabel 32 Eisen uit de BIO t.a.v. cryptografie

Fysieke beveiliging en beveiliging van de omgeving	
11.2.1	Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.

Tabel 33 Eisen uit de BIO t.a.v. fysieke beveiliging en beveiliging van de omgeving

Beveiliging bedrijfsvoering	
12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.
12.1.3	Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.
12.1.4	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.
12.2.1	Ter bescherming tegen virussen, malware, ransomware, etc. behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, dit in combinatie met een passend bewustzijn van gebruikers.
12.3.1	Regelmatig behoren back-upkopieën van informatie, software en systeemaafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid. Hierbij is op basis van een expliciete risicoafweging bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.
12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. Een logregel bevat minimaal: a) De gebeurtenis; b) De benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; c) Het gebruikte apparaat; d) Het resultaat van de handeling; e) Een datum en tijdstip van de gebeurtenis.
12.4.2	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
12.4.3	Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
12.5.1	Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd, zodat wordt voorkomen dat ongewenste software als virussen, malware, ransomware, etc. wordt geïnstalleerd.
12.6.1	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.

Tabel 34 Eisen uit de BIO t.a.v. beveiliging bedrijfsvoering

Communicatiebeveiliging	
13.1.1	Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
13.1.2	Beveiligingsmechanismen, dienstverleningsniveaus en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
13.2.1	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
13.2.2	Overeenkomsten over informatietransport behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.

13.2.3	Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.
---------------	---

Tabel 35 Eisen uit de BIO t.a.v. communicatiebeveiliging

Acquisitie, ontwikkeling en onderhoud van informatiesystemen	
14.1.1	De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.
14.1.2	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.
14.2.2	Procedures voor wijzigingsbeheer m.b.t. systemen: Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.
14.2.8	Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.
14.2.9	Systeemacceptatietests: Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.
14.3.1	Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.

Tabel 36 Eisen uit de BIO t.a.v. acquisitie, ontwikkeling en onderhoud van informatiesystemen

Leveranciersrelaties	
15.2.1	Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen. Vanuit de NIS2 is vereist dat leveranciers in de leveranciersketen een letter of compliance afgeven met daarin beveiligingsclausules over bijvoorbeeld meldingsverplichtingen bij incidenten, audit/rechten tot inspectie, doorstroom (flow-down) van verplichtingen naar sub-leveranciers, exit- of sanctierechten, etc.

Tabel 37 Eisen uit de BIO t.a.v. leveranciersrelaties

Beheer van informatiebeveiligingsincidenten	
16.1.2	Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
16.1.5	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
16.1.6	Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen, behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.
16.1.7	De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.

Tabel 38 Eisen uit de BIO t.a.v. beheer van informatiebeveiligingsincidenten

Naleving	
18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

Tabel 39 Eisen uit de BIO t.a.v. naleving

8.1. Aanvullende eisen vanuit de NIS2

Er is een nieuwe Europese richtlijn voor informatiebeveiliging (NIS2). Behalve de klassieke beveiligingsmaatregelen die al vanuit de BIO gelden, richt de NIS2 zich ook nadrukkelijker op een aantal governance-achtige aspecten, zoals de melding van beveiligingsincidenten (ook door de ketens heen), het compliant zijn van leveranciers van informatievoorzieningen, etc.

Belangrijke aanvullende eisen van de NIS2 richtlijn zijn onder meer:

- **Strengere eisen:**
Er worden strengere eisen gesteld aan de beveiliging van netwerk- en informatiesystemen.
- **Ketenzorgplicht: incidenten voorkomen en maatregelen nemen**
Aanbieders van essentiële diensten en digitale dienstverleners zijn verplicht om niet alleen hun eigen cybersecurity te waarborgen, maar ook actief bij te dragen aan de beveiliging van de gehele keten waar zij deel van uitmaken en zij moeten technische en organisatorische maatregelen nemen om hun netwerk- en informatiesystemen te beveiligen. Dit houdt in dat zij verantwoordelijkheden hebben t.a.v. de digitale veiligheid van hun partners en leveranciers. Die maatregelen moeten passend en evenredig zijn.
- Verder nemen zij passende maatregelen om incidenten te voorkomen en – als zich toch incidenten voordoen – de gevolgen daarvan zo veel mogelijk te beperken. Onder een incident verstaan we een gebeurtenis met schadelijke effecten op de beveiliging van netwerk- en informatiesystemen, met aanzienlijke verstoring van de dienstverlening tot gevolg. Bij de beveiliging van netwerk- en informatiesystemen gaat het om de beschikbaarheid, integriteit, vertrouwelijkheid, en authenticiteit (biva) van netwerk- en informatiesystemen.
- **Meldplicht: Incidenten melden**
Er is een meldplicht voor incidenten. Dit betekent dat als er iets misgaat, dit moet worden gemeld bij de relevante autoriteiten. In Nederland moet dit worden gemeld bij de Rijksinspectie Digitale Infrastructuur (RDI) en bij een Computer Security Incident Response Team (CSIRT). Voor aanbieders van essentiële diensten is het NCSC het aangewezen CSIRT. Digitale dienstverleners schakelen het CSIRT-DSP in.
- **Toezicht en handhaving:**
Er worden maatregelen ingevoerd om de naleving van de NIS2 richtlijn te verzekeren, inclusief financiële sancties voor niet-naleving. De Rijksinspectie Digitale Infrastructuur (RDI¹⁸) is in Nederland de toezichthouder op de naleving van de Wbni (de Nederlandse implementatie van de NIS2) voor o.a. overheids- en digitale dienstverleners. Dit toezicht geldt voor zowel de zorgplicht als voor de meldplicht die op organisaties rust.
 - Toezicht op aanbieders van essentiële diensten.
 - Deze groep aanbieders valt onder een actief toezichtbeleid. Er vinden geplande inspecties plaats, gericht op het risicomanagementproces en het treffen van passende beheersingsmaatregelen. Daarbij worden ook reality checks uitgevoerd.
 - Toezicht op digitale dienstverleners.
 - Bij deze aanbieders wordt een reactief toezicht gehanteerd. Inspecties vinden plaats op basis van signalen en incidenten. De RDI heeft, net als andere toezichthouders, bij de uitvoering van het toezicht diverse bevoegdheden. Zoals het (laten) uitvoeren van een beveiligingsinspectie. Ook heeft de RDI de mogelijkheid om handhavend op te treden.

8.2. Eisen vanuit de BIO2 t.a.v. de gebruikte gegevens

De meest essentiële van toepassing zijnde maatregelen vanuit de BIO2 zijn hieronder opgesomd.

Informatiebeveiligingsbeleid	
5.08.01	Bij nieuwe informatiesystemen en bij significante wijzigingen op bestaande informatiesystemen wordt een expliciete risicoafweging op basis van een vastgestelde risicomanagementmethodiek uitgevoerd, om risico's te identificeren en in voldoende mate te beheersen en ook voor het vaststellen van de beveiligingseisen.

¹⁸ [Wet beveiliging netwerk- en informatiesystemen \(Wbni\) | Rijksinspectie Digitale Infrastructuur \(RDI\)](#)

5.09.01	- De inventaris van bedrijfsmiddelen omvat alle eigenschappen die nodig zijn voor het beheer en onderhoud. In de inventaris zijn ook opgenomen: bedrijfsmiddelen op afstand, cloud-omgevingen en bedrijfsmiddelen die regelmatig zijn verbonden met de netwerkinfrastructuur maar niet onder controle van de entiteit staan. - De volledigheid en actualiteit van de inventaris van bedrijfsmiddelen wordt periodiek gecontroleerd met tussenpozen die passend zijn voor de frequentie waarmee wijzigingen optreden.
5.10.03	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.
5.12.01	Informatie in alle informatiesystemen wordt met een expliciete risicoafweging geclassificeerd. Hierbij wordt gebruik gemaakt van een vastgestelde impactclassificatiemethodiek die onderdeel is van de vastgestelde risicomanagementmethodiek.
5.14.02	De entiteit maakt bij openbaar webverkeer van gevoelige gegevens gebruik van ten minste publiek vertrouwde Organization Validated (OV)-certificaten.
5.14.04	Van alle internetfacing-informatiesystemen, webapplicaties, IP-adressen en API's is er een actuele registratie.
5.14.05	Publiek toegankelijke websites worden bekend gemaakt via het Register Internetdomeinen Overheid (RIO). Deze informatie wordt ten minste iedere zes maanden geactualiseerd.
5.15.01	Toegang tot een vertrouwde zone is toegestaan in twee situaties: 1. vanaf geauthentiseerde apparatuur of; 2. vanuit programmatuur die draait binnen een veilige schil.
5.16.01	Er is een sluitende formele registratie- en afmeldprocedure voor het beheeren van gebruikersidentificaties.
5.18.01	Het maken en aanpassen van accounts met bijzondere rechten wordt gemonitord. Indien deze wijzigingen ongeautoriseerd zijn, is dit een informatiebeveiligingsincident en wordt dat als zodanig vastgelegd en afgehandeld.
5.19.01	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, zijn informatiebeveiligingseisen waaronder de beschikbaarheid, integriteit en vertrouwelijkheid, onderdeel van het hele pakket aan inkoopseisen. De informatiebeveiligingseisen zijn gebaseerd op een expliciete risicoafweging.
5.20.01	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in (inkoop)contracten waar de verwerking van informatie een rol speelt.
5.20.03	In het beschrijvend document wordt opgenomen dat de leverancier aantoont dat hij aan alle gestelde eisen voldoet in opzet, bestaan en werking, op basis van onderzoeken van onafhankelijke derden. Deze onderzoeken hebben een scope die dekkend is voor de gecontracteerde dienstverlening. Hierbij is expliciet aandacht voor de toeleveringsketen en hoe de leverancier zijn leveranciersmanagement ingeregeld heeft. Dit toont de leverancier jaarlijks opnieuw aan.
5.20.05	Onderdeel van de afspraken is dat de leverancier transparant is over kwetsbaarheden in de dienstverlening en informatiebeveiligingsincidenten waaronder datalekken. Dit stelt de entiteit in staat om passend te reageren onder meer door te rapporteren en mitigerende maatregelen te nemen.
5.21.03	De entiteit borgt dat de beveiligingseisen aan de leverancier onverminderd van toepassing zijn op de keten van toeleveranciers, tenzij die eisen niet relevant zijn gezien de aard van de dienstverlening door de toeleverancier.

5.27.01	Informatiebeveiligingsincidenten worden geanalyseerd om achterliggende oorzaken vast te stellen, verbeteringen te realiseren, om zo toekomstige incidenten te voorkomen.
5.27.02	De analyses van informatiebeveiligingsincidenten, inclusief de achterliggende oorzaken en de verbeteringen worden breed gedeeld met relevante partners om herhaling en toekomstige incidenten te voorkomen.
5.33.01	De proceseigenaar heeft voor alle informatie(systemen) in selectielijsten de bewaartermijn vastgelegd, rekening houdend met de eigen bedrijfsdoelstellingen en wet- en regeling, zoals de archiefwet en privacywetgeving.
8.07.01	Het downloaden van bestanden is beheerst en beperkt op basis van het risico en need-of-use. De antimalware-software beoordeelt altijd alle downloads.
8.07.04	De malwarescan wordt uitgevoerd op: • alle gedownloade content voorafgaand aan executie of opslag; • alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik of opslag in de eigen omgeving.
8.13.01	Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld. Er is speciale aandacht voor het beschermen van de back-up tegen ransomware-aanvallen en genomen maatregelen om de integriteit van de back-up te behouden.
8.15.01	Een logregel bevat minimaal: a) Actie: de gebeurtenis of handeling die heeft plaatsgevonden. b) Object: waarop de gebeurtenis of handeling effect had (bijvoorbeeld welk bestand, proces of systeem). c) Resultaat: het resultaat van de gebeurtenis of handeling. d) Oorsprong: het apparaat of de netwerklocatie van waaruit de gebeurtenis of handeling in gang is gezet. e) Actor: identificatie van de persoon die of het proces dat de gebeurtenis in gang heeft gezet. f) Tijdstempel: datum en tijdstip waarop de gebeurtenis of handeling plaatsvond.
8.15.05	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als informatiebeveiligingsincident via de procedure voor informatiebeveiligingsincidenten volgens beheersmaatregel 5.24 uit NEN-EN-ISO/IEC 27002:2022.
8.24.01	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: a) Wanneer cryptografie ingezet wordt. b) Wie verantwoordelijk is voor de implementatie. c) Wie verantwoordelijk is voor het sleutelbeheer. d) Hoe geregistreerd wordt waar welke cryptografie toegepast wordt. e) Welke normen als basis dienen voor cryptografie en de wijze waarop de passende normen van het Forum Standaardisatie worden toegepast. f) De wijze waarop het beschermingsniveau vastgesteld wordt. g) Bij communicatie tussen entiteiten wordt het beleid onderling vastgesteld.
8.27.01	Architectuurprincipes zoals 'security by design' en 'security by default' voor het ontwerpen van de beveiliging van informatiesystemen worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten over het ontwikkelen van informatiesystemen.

Tabel 40 Eisen uit de BIO2 t.a.v. informatiebeveiliging

Bijlagen

Bijlage: Index met gebruikte afkortingen en begrippenlijst

Afkorting	Beschrijving	Omschrijving
AI-act	EU-wetgeving rondom Artificial Intelligence	EU AI Act: first regulation on artificial intelligence Topics European Parliament (europa.eu) Regels AI-modellen voor algemene doeleinden - Digitale Overheid
API	Application Programming Interface	Een API is een afgesproken manier waarop software met andere software praat.
BBN2	Basisbeveiligingniveaus	De Baseline Informatiebeveiliging Overheid (BIO) kent drie basisbeveiligingniveaus, ook wel BBN's genoemd. Voor de meeste informatiesystemen is BBN2 voldoende. Een Basis Beveiligings Niveau (BBN) is een verzameling van een minimale set van passende maatregelen om een bepaald belang te beschermen. Binnen de BIO kennen we drie (oorspronkelijke) BBN's met bijbehorende beveiligingseisen, namelijk BBN1, BBN2, BBN3 en aanvullend voor gemeenten is er ook nog BBN2+. • BBN1 is het minimale niveau waar alle informatiesystemen aan moeten voldoen op basis van de geldende wet- en regelgeving en algemene beveiligingsprincipes. • BBN2 is het uitgangspunt voor alle informatiesystemen. Dit BBN is van toepassing op het moment dat er vertrouwelijke informatie wordt verwerkt, mogelijke incidenten kunnen leiden tot bestuurlijke commotie, er onzekerheid bestaat of ook alle informatie van derden open is en de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem. • BBN3 richt zich op de bescherming van Departementaal Vertrouwelijk gecategoriseerde informatie, waarbij weerstand geboden moet worden tegen een statelijke dreiging/actoren. BBN3 wordt binnen gemeenten eigenlijk niet toegepast, of je moet als gemeente bijv. met de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) samenwerken. • BBN2+ is in het leven geroepen omdat het voor gemeenten soms noodzakelijk is om aanvullende maatregelen te nemen boven BBN2. Het is dus een passende set van maatregelen bovenop BBN2. Bovenstaande BBN's zijn uitgewerkt langs de bekende lijnen van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Elke BBN bestaat uit een aantal controls, verplichte maatregelen en een verantwoordings- en toezichtsregime.¹⁹

¹⁹ [Wanneer gebruik je BBN2+? - Informatiebeveiliging & Privacy \(ib-p.nl\)](#)

BIO	Baseline Informatiebeveiliging Overheid	Home NL - bio-overheid , ICO Wizard - bio-overheid
DPIA	Data Protection Impact Assessment	Als er met persoonsgegevens wordt verwerkt en alle te realiseren informatievoorzieningen moeten voldoen aan de privacywetgeving, moeten DPIA's worden uitgevoerd. Dit beleid wordt getoetst d.m.v. het uitvoeren van DPIA's: • Periodiek bij het in gebruik zijn van de informatievoorzieningen. • Na de ontwerpfase van de gewenste veranderingen t.a.v. voorzieningen in de processen en de daarmee gerelateerde ondersteunende informatievoorzieningen, • Na het opleveren van de gewenste veranderingen in de processen en de daarmee gerelateerde ondersteunende informatievoorzieningen en • Periodiek bij het in gebruik zijn van de informatievoorzieningen bij de werking in de processen. De geïdentificeerde risico's en aanbevelingen vanuit de DPIA moeten worden vertaald naar maatregelen om die risico's terug te brengen naar acceptabele niveaus. Deze maatregelen moeten worden geïmplementeerd bij de realisatie van ondersteunende voorzieningen bij de vastlegging en verwerking van die persoonsgegevens, zodat de verwerking van persoonsgegevens compliant is aan de wetgeving.
Hosting		Het beschikbaar stellen en in productie houden van het systeem.
Housing		De accommodatie waarin centrale ICT-infrastructuur ondergebracht kan worden.
NIS2	Network and Information Security Directive 2	De NIS2 is een Europese wetgeving die lidstaten verplicht om hun nationale cybersecuritymaatregelen aan te scherpen. Het doel is om een hoog gemeenschappelijk niveau van cyberbeveiliging in de hele EU te realiseren. Belangrijke verplichtingen onder de NIS2 1. Risicobeheer en beveiliging: Organisaties moeten passende technische en organisatorische maatregelen nemen (zoals risicoanalyses, incidentdetectie, business continuity, encryptie, etc.). 2. Meldplicht voor incidenten: Ernstige beveiligingsincidenten moeten binnen 24 uur worden gemeld aan de nationale toezichthouder. 3. Toezicht en handhaving: Nationale autoriteiten (in Nederland: het Digital Trust Center of de NCTV, afhankelijk van de sector) krijgen bevoegdheden om audits uit te voeren en sancties op te leggen. 4. Bestuurdersverantwoordelijkheid: Bestuurders zijn expliciet verantwoordelijk voor het naleven van NIS2-maatregelen en kunnen persoonlijk aansprakelijk worden gesteld bij nalatigheid.

		5. Leveranciersketenbeheer: Organisaties moeten ook risico's in hun toeleveringsketen beheren en beoordelen.
NORA	Nederlandse Overheid Referentie Architectuur	Het is een kaderset en referentiearchitectuur die bedoeld is om overheidsorganisaties in Nederland te helpen bij het inrichten van hun digitale dienstverlening en ICT-architectuur. NORA is een belangrijk hulpmiddel voor bijvoorbeeld IT-architecten, informatiemanagers, beleidsmakers en projectleiders binnen de overheid.
SLA	Service Level Agreement	Overeenkomst tussen de opdrachtnemer en de opdrachtgever. In een SLA wordt afgesproken wat de prestatie-indicatoren en kwaliteitseisen zijn van de te leveren dienst of product, om deze later te kunnen toetsen. In een SLA worden de rechten en plichten van beide partijen omschreven. Aanvullend op de SLA is het DAP opgesteld, waarin afspraken staan over de manier van samenwerking tussen aanbieder en afnemer. De SLA en DAP vormen samen met evt. addenda de samenwerkingsafspraken.

Tabel 41 Index met gebruikte afkortingen en begrippenlijst