# ROSA Architectuurscan/advies: Dienst Verwerkersovereenkomsten

| | |
|---|---|
| **Voor** | Architectuurraad |
| **Van** | Bureau Edustandaard |
| **Scan uitgevoerd door** | Remco de Boer |
| **Versie** | 2e concept |
| **Datum** | 31 jan 2023 |
| **Versiehistorie** | 1e concept: opgesteld door BES<br>2e concept: afgestemd met de indiener en direct betrokkenen<br>definitief: behandeld door Architectuurraad |
| **Aanleiding** | Verzoek ROSA-scan Dienst Verwerkersovereenkomsten |
| **Betreft** | Dienst Verwerkersovereenkomsten |
| **Brondocument(en)** | PRD Dienst Verwerkersovereenkomst, v1.0, 21-10-2022 |
| **Begeleidende documenten** | Pitchdocument Dienst Verwerkersovereenkomsten, aug. 2022<br>Voorstel Governance Dienst verwerkersovereenkomsten v1.1, 26 sep. 2022 |

## Inleiding

Met de ROSA Architectuurscan worden op systematische wijze alle architectuuraspecten van een bij Edustandaard ingebracht onderwerp in kaart gebracht en worden knelpunten en kansen gesignaleerd. Niet alleen kan de indiener er zijn voordeel mee doen, ook kan ROSA ermee worden verrijkt. En tot slot stelt het andere ketenpartijen in staat om kennis te nemen van architectuurwijzigingen en het belang hiervan voor de eigen organisatie of achterban te bepalen (transparantie in de keten, informatiepositie).

Dit formulier bevat de uitkomst van een architectuurscan van het **Dienst Verwerkersovereenkomsten**. Voor de indiener biedt de scan concrete handvatten voor toepassing van ROSA, en de mogelijkheid om lessen en ervaringen uit het project terug te koppelen aan ROSA. Een architectuurscan wordt in principe uitgevoerd met een hoge mate van betrokkenheid van vertegenwoordigers van de inbrenger. Deze wordt hierbij ondersteund door Bureau Edustandaard, de beheerder van ROSA. De inbrenger zou zich moeten herkennen in de uitkomsten.

Iedere architectuurscan begint met de vraag: welke onderdelen van ROSA zijn relevant voor het ingebrachte onderwerp, en indien relevant, op welke wijze? Vervolgens worden de vragen gesteld hoe het ingebrachte past op wat in ROSA is uitgewerkt, en of het project wellicht inzichten heeft die kunnen leiden tot verbetering of uitbreiding van ROSA. De antwoorden op deze vragen worden verwoord in termen van een advies richting zowel inbrenger, als richting ROSA zelf. De opzet van het advies is dat per onderdeel van ROSA uitspraken worden gedaan over:

1. Bevindingen uit project: *wat zegt het project zelf over het verband met ROSA van het ingebrachte onderwerp?*
2. Relatie met ROSA: *hoe verhoudt het ingebrachte zich tot ROSA[1]?*
3. Voorgesteld advies van de Architectuurraad aan het project: *tips, verbeterpunten, en ook bekrachtiging dat er goed werk is geleverd vanuit het perspectief van ROSA[2]*
   Adviezen in deze kolom zijn, gegroepeerd in 'PRODUCT' en 'CONTEXT'. De PRODUCT-adviezen bestrijken sec het ingediende 'product', d.w.z. **Dienst Verwerkersovereenkomsten**. Deze adviezen zijn direct gericht aan de project(deel)groep die zich met de totstandkoming van **Dienst Verwerkersovereenkomsten** bezighoudt. De CONTEXT-adviezen hebben betrekking op de context waarbinnen **Dienst Verwerkersovereenkomsten** toegepast gaat worden. Deze adviezen kunnen gericht zijn aan het project zelf, maar kunnen ook zijn gericht aan partijen die zich in die context bevinden, zoals de project(deel)groep die zich richt op de implementatie van de uiteindelijke **Dienst Verwerkersovereenkomsten**, maar ook (sector)organisaties die met de uiteindelijke implementatie te maken gaan krijgen.
4. **Voorgesteld advies voor de Architectuurraad voor plaatsing onderwerpen op de ROSA architectuur backlo**g: *wat kan ROSA doen om in het vervolg een betere ondersteuning te bieden aan dit project, en andere?*

Samenhang met andere formulieren:

- **Pitch Architectuurscan**: Het doel van de architectuurpitch is om een eerste indruk te krijgen van een ketenafspraak . Op basis van de pitch en de aangeleverde documentatie voert Bureau Edustandaard een architectuurscan uit. Voor de leden van de Architectuurraad (en andere geïnteresseerden) verduidelijkt deze pitch de context van de afspraak en de resultaten uit de architectuurscan.
- **ROSA architectuurscan *bevindingen***: aan het invullen van het adviesdeel van een architectuurscan (dit formulier) gaat het verzamelen van feitelijke informatie, en het analyseren daarvan, vooraf. Die informatie, en de analyses, worden vastgelegd in het bevindingendeel van de architectuurscan. De lezer van het adviesdeel kan die erop na slaan als hij wil weten hoe het advies tot stand is gekomen. Het lezen van het bevindingendeel is niet vereist om het adviesdeel te begrijpen. Waar van toepassingen verwijst het bevindingendeel naar specifieke locaties van de brondocumenten die als input dienden voor de architectuurscan. Ook het lezen van de brondocumenten is niet vereist om het adviesdeel te begrijpen.

[1] De verhouding tussen het ingediende en de ROSA wordt per onderdeel uitgedrukt in een 'level of conformance' ontleend aan TOGAF, zie de bijlage.
[2] Dit is een concept advies, de uitkomsten worden eerst door de Architectuurraad besproken.

# ROSA Architectuurscan/advies: Dienst Verwerkersovereenkomsten

| ROSA-onderdeel | Bevindingen uit project: Dienst Verwerkersovereenkomsten | Relatie met ROSA (blauw: ROSA, geel: Dienst Verwerkersovereenkomsten) | Voorgesteld advies aan project | Voorgesteld advies aan AR voor plaatsing onderwerpen op de architectuurbacklog ROSA |
|---|---|---|---|---|
| **Werkingsgebied** | Het pitchdocument positioneert de Dienst Verwerkersovereenkomsten als “basisvoorziening voor het funderend onderwijs”. |  **Compliant –** het werkingsgebied (funderend onderwijs) valt binnen de reikwijdte van ROSA c.q. het werkingsgebied onderwijs. | **PRODUCT:**<br>**CONTEXT:** | |
| **Ketendomeinen en -processen** | |  **Irrelevant** – De dienst is niet gericht op specifieke ketendomeinen en/of -processen, maar ondersteunt de invulling van een randvoorwaarde (het zorgen voor ondertekende verwerkersovereenkomsten) die geldt voor alle ketenprocessen waarin verwerking door verwerkers plaatsvindt. | **PRODUCT:**<br>**CONTEXT:** | |
| **Scenario** | “De dienst verwerkersovereenkomsten brengt leveranciers en schoolbesturen samen en stelt hen in staat om onderling in een besloten omgeving hun verwerkersovereenkomsten met elkaar af te stemmen en te ondertekenen. Daarnaast biedt het beiden overzicht van alle verwerkersovereenkomsten die zijn afgesloten.” |  **Onbepaald** – De Dienst Verwerkersovereenkom-sten valt binnen het IV-domein Inrichten IBP. In dit IV-domein is o.a. de relatie tussen verwerker en verwerkingsverantwoordelijke uitgewerkt in relatie tot een Gegevensverwerkend Systeem. De relatie tussen (de modellen in) het PRD en het IV-domein in | **PRODUCT:**<br>**CONTEXT:** | |

| | | | | |
|---|---|---|---|---|
| | | ROSA zijn in het PRD niet verder uitgewerkt of toegelicht. | | |
| ***Ontwerpgebied***<br><br>**Effectieve ketengovernance** | Paragraaf 1.2 van het PRD geeft een overzicht van interne en externe belanghebbenden en de rollen die zij t.o.v. de (ontwikkeling van de) voorziening hebben. In het *Voorstel Governance* is in meer detail een governancestructuur uitgewerkt inclusief verantwoordelijkheden en aansluitvoorwaarden. |  **Compliant** – Binnen het project is zicht op de belanghebbenden en de wijze waarop zij betrokken worden.<br><br>*Kanttekening* ten aanzien van het ontwerpkader ***Bewaak relaties met andere afspraken*** – in het PRD worden verschillende afhankelijkheden benoemd tussen de Dienst Verwerkersovereenkomsten en andere (soms nog te ontwikkelen) voorzieningen. Het is onduidelijk hoe de afstemming voor deze afhankelijkheden vormgegeven is of wordt. Op dit onderdeel dus: Onbekend. | **PRODUCT:** Werk verder uit hoe de afstemming met gerelateerde voorzieningen als onderdeel van 'het platform' is of wordt ingericht.<br><br>**CONTEXT:** | |
| ***Ontwerpgebied***<br><br>**Ketenbrede informatiebeveiliging en privacybescherming** | Het PRD omvat een BIV-classificatie en een beschrijving van de te nemen beheersmaatregelen. |  **Compliant** – Geeft invulling aan de ontwerpkaders uit het ontwerpgebied IBP. | **PRODUCT:**<br>De dienst krijgt een B-score '2' omdat een verstoring van het ondertekenproces het primaire proces niet verstoort. Dit verandert sterk wanneer, zoals in het PRD wordt geschetst, de voorziening in de toekomst een operationele rol zou krijgen in uitwisselprocessen (check getekende | |

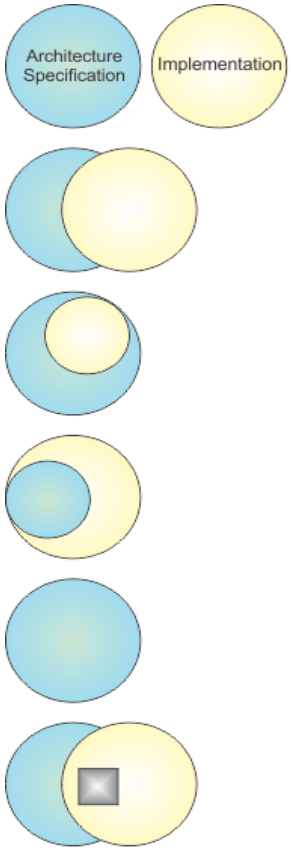
| | | | | |
|---|---|---|---|---|
| | | | verwerkersovereenkomst bij afgeven mandaat).<br><br>Sommige maatregelen vergen nadere uitwerking. Zo wordt gesteld dat “De bewaartermijn voor persoonlijke gegevens wordt vastgelegd en automatisch gehandhaafd” wat vraagt om een verdere duiding van het handhavingsproces. Ook wordt bijvoorbeeld gesteld dat “toegang tot systemen en gegevens tot het minimum beperkt wordt”, wat vraagt om een specificatie wat dat ‘minimum’ is.<br><br>**CONTEXT:** | |
| ***Ontwerpgebied***<br><br>**Ketenbrede interoperabiliteit** | Afbeelding 7 toont een informatiemodel met gegevensentiteiten voor de Dienst Verwerkersovereenkomsten. Hierin staan o.a. de volgende elementen:<br>• Onderwijsinstelling<br>• Leverancier<br>• Verwerkingsactiviteit<br>• Digitaal onderwijsmiddel (product/dienst)<br>• Verwerkersovereenkomst<br>Definities bij de entiteiten ontbreken. | **Explain** –<br>Het model impliceert dat de Onderwijsinstelling optreedt als verwerkingsverantwoordelijke, terwijl in de tekst van het PRD op het Bestuur als verwerkingsverantwoordelijke wordt benoemd.<br><br>Het model impliceert dat Verwerkingsactiviteiten in de voorziening worden geregistreerd, waar in de tekst wordt aangegeven dat dat niet zo is.<br><br>De entiteiten in het informatiemodel zijn gerelateerd | **PRODUCT:**<br>Hanteer eenduidige begrippen (bestuur vs. onderwijsinstelling).<br><br>Verduidelijk de scope van de voorziening Verwerkersovereenkomsten (zie ook het onderdeel Referentiecomponenten en Ketenvoorzieningen)<br><br>Voeg definities toe bij modelelementen.<br><br>Licht de relatie met ROSA (en FORA) toe en stem waar nodig de modellen verder af op het ROSA | |

| | | | | |
|---|---|---|---|---|
| | | aan entiteiten uit het ROSA IV-domein IBP, het FORA Informatiemodel Bedrijfsvoering (geen onderdeel van deze scan), en begrippen uit het ROSA Begrippenkader. Er is niet uitgewerkt in hoeverre deze modellen als uitgangspunt gebruikt zijn.<br><br>De entiteiten zijn ook gerelateerd aan het Gemeenschappelijk Informatiemodel voor Voorzieningen dat is opgenomen in NORA, en mede voortkomt uit de Softwarecatalogus/Dienst Product Catalogus casus in het onderwijs. Het is onduidelijk in hoeverre dit model, en het bijbehorende uitgangspunt dat deze use case vooral een dataintegratievraagstuk betreft, zijn weerslag heeft in de opzet van de Dienst Verwerkersovereenkomsten. | Begrippenkader en IV-domein IBP.<br><br>Verduidelijk hoe de Dienst Verwerkersovereenkomsten aansluit bij het Gemeenschappelijk Informatiemodel voor Voorzieningen en de achterliggende idee dat deze en andere use cases primair een data-integratie-vraagstuk betreffen (zie ook het onderdeel Referentiecomponenten en ketenvoorzieningen)<br><br>**CONTEXT:** | |
| ***Ontwerpgebied***<br><br>**Ketenbrede toegankelijkheid** | De dienst zal gebruik maken van eHerkenning voor toegang en ondertekenen. Daarnaast zal/zullen (delen van?) de dienst toegankelijk zijn via Entree. Beheerders van de dienst maken binnen Kennisnet gebruik van een eigen, interne, SSO-voorziening obv ADFS. | **Onbepaald** – er moet nog worden bepaald welke rollen er worden onderscheiden en welk (eHerkenning-)betrouwbaarheidsniveau daarbij moet worden gehanteerd. Het schema in Afb. 14 toont een stap waarin een inlogmethode wordt geselecteerd (eHerkenning of Entree). In de tekst wordt niet toegelicht wanneer / voor welke functies of delen van de dienst Entree gebruikt kan worden. | **PRODUCT:**<br>Verhelder de selectie van inlogmethode, in het bijzonder in welke gevallen er gebruik gemaakt kan worden van Entree.<br><br>Werk de rollen en benodigde betrouwbaarheidsniveaus verder uit.<br><br>**CONTEXT:** | |

| | | | | |
|---|---|---|---|---|
| **Referentie-componenten en ketenvoorzieningen** | Paragraaf 3.2 stelt dat de componenten een mogelijk toekomstbeeld schetsen, maar dat in de huidige opzet het de bedoeling is dat alleen verwerkersovereenkomsten worden geregistreerd.<br><br>De mapping op FORA in diezelfde paragraaf is heel breed, en benoemt o.a. invulling van 'registratie van verwerkingsactiviteiten' als functie die door de voorziening wordt ondersteund.<br><br>Afb. 5 (e.v.) toont verschillende doelen, waaronder 'Applicatielandschap inzichtelijk maken'.<br><br>Afb. 6 toont dat diverse gerelateerde functies die geleverd moeten worden door verschillende voorzieningen (Dienst Verwerkersovereenkomsten, Dienst Product Catalogus, Kennisnet Authenticatiehub, Interne Registers en Kantoorautomatisering) samen invulling geven aan het 'gesloten domein'.<br><br>Afb. 15 toont een fasering voor oplevering van verschillende componenten. |  **Explain** - De beoogde functionaliteit is niet altijd eenduidig beschreven. De functie 'Registratie verwerkingsactiviteiten' (par 3.2) is in tegenspraak met de beperking tot registratie van verwerkersovereenkomsten.<br><br>Het doel 'Applicatielandschap inzichtelijk maken' genoemd in Afb. 5 e.v. lijkt geen doel van de Dienst Verwerkersovereenkomsten, maar eerder van de in het PRD benoemde (gerelateerde) voorziening Softwarecatalogus/Dienst Product Catalogus.<br><br>De onderlinge afhankelijkheden tussen de verschillende voorzieningen behoeft verdere uitwerking. Het is bijv. verwarrend dat in Afbeelding 15 functionaliteiten en gegevens die bij de Dienst Product Catalogus horen, in scope van het MVP van de Dienst Verwerkersovereenkomsten worden geplaatst. | **PRODUCT:**<br>Maak een duidelijk onderscheid tussen componenten en functies die in scope zijn van de Dienst Verwerkersoveenkomsten en functies die buiten scope zijn waarnaar een afhankelijkheid bestaat. Koppel daar een roadmap aan die duidelijk maakt welke functionaliteiten op welk moment waar worden gerealiseerd, met aandacht voor een evt. transitie indien de functionaliteit pas op een later moment op de juiste plaats kan worden belegd. (Zie ook de kanttekening bij het onderdeel 'Governance' in deze scan).<br><br>De FORA-mapping lijkt heel breed; waar deze voorziening in essentie (alleen/vooral) over Contractbeheer gaat. (NB. Deze scan beoogt geen volledige scan t.o.v. FORA te zijn).<br><br>**CONTEXT:** | |
| **Beheer en (door)ont-wikkeling** | | | **PRODUCT:**<br><br>**CONTEXT:** | |

| Implementatie | | | PRODUCT:<br>CONTEXT: | |
|---|---|---|---|---|

# Bijlage 1: ARCHITECTURE COMPLIANCE (TOGAF)




**Irrelevant:**
The implementation has no features in common with the architecture specification (so the question of conformance does not arise).

**Consistent:**
The implementation has some features in common with the architecture specification, and those common features are implemented in accordance with the specification. However, some features in the architecture specification are not implemented, and the implementation has other features that are not covered by the specification.

**Compliant:**
Some features in the architecture specification are not implemented, but all features implemented are covered by the specification, and in accordance with it.

**Conformant:**
All the features in the architecture specification are implemented in accordance with the specification, but some more features are implemented that are not in accordance with it.

**Fully Conformant:**
There is full correspondence between architecture specification and implementation. All specified features are implemented in accordance with the specification, and there are no features implemented that are not covered by the specification.

**Non-conformant:**
Any of the above in which some features in the architecture specification are implemented not in accordance with the specification.



Een Nederlandse vertaling van de beschrijving van de TOGAF-categorieen:

- **irrelevant** = er is geen relatie tussen het ingebrachte en ROSA
- **consistent** = er is overlap tussen het ingebrachte en ROSA, en binnen die overlap is het ingebrachte conform ROSA gerealiseerd, de overlap is echter niet **volledig** = sommige specificaties van ROSA zijn niet overgenomen, en het ingebrachte heeft onderdelen die niet door ROSA worden gedekt.
- **compliant** = het ingebrachte valt volledig binnen ROSA (subset) en is conform ROSA gerealiseerd
- **conformant** = ROSA dekt alleen een deel van het ingebrachte, maar dat deel is wel conform ROSA gerealiseerd
- **fully conformant** = ROSA dekt het geheel van het ingebrachte, en niets van het ingebrachte valt buiten ROSA
- **non-conformant** = er is overlap tussen het ingebrachte en ROSA, en binnen die overlap is er iets van het ingebrachte *niet* conform ROSA gerealiseerd

Bron: http://pubs.opengroup.org/architecture/togaf9-doc/arch/Figures/48_conformance.png