



Data.OD

ARCHITECTUUR DATA.OD

Aspecten Compliancy by Design

- E: Stuurgroep Data.OD
- B: Architect
- Versie 0.9
- 10 juni 2026

Samenwerking van I-Go en DCMR



De kernvraag is hoe we Data.OD technisch en inhoudelijk kunnen laten versnellen, terwijl rechtmatigheid, privacy en security in de basis zijn ingeregeld en niet pas achteraf worden gerepareerd.

Wat vanuit ISO minimaal geborgd moet zijn vóór ingebruikname

- Formele rol en verantwoordelijkheidsverdeling (ketenbreed).
- Bron specifieke afspraken over classificatie, grondslag, bewaartermijn en hergebruik.
- Keten BIO maatregelen (IAM, logging, incidentafhandeling, auditability).
- Privacy borging vóór implementatie (DPIA gekoppeld aan ontwerp).
- Heldere positionering van OD's: wat wordt lokaal verwerkt, wat niet, en waarom.

Bij een hack zijn de OD's (individueel of gezamenlijk) juridisch verantwoordelijk. Data.OD (als beheerorganisatie) voert uit maar is nooit verantwoordelijk onder de AVG.

KERNONDERWERPEN

1. Rechtmatigheid
2. Rolvaststelling
3. Verwerkersovereenkomsten
4. Ketenrisico
5. Incident & response
6. Bronspecifieke afspraken
7. (Pré) DPIA
8. Governance
9. Overige security aspecten
10. Overige privacy aspecten
11. Archivering



1. RECHTMATIGHEID

➤ **De rechtmatigheid van Data.OD moet eenduidig en transparant beschreven zijn.**

Hierin moeten o.a. de volgende aspecten duidelijk naar voren komen:

- Waar ligt de juridische grondslag
- Hoe Data.OD wordt gepositioneerd
- Hoe de rechtmatigheid per databron en per gebruiksdoel wordt vastgesteld en geborgd

De kernvraag over rechtmatigheid is richtinggevend voor alle andere vragen en keuzes rondom Data.OD

Waar ligt de juridische grondslag:

- Bij Data.OD als initiatief?
- Bij de wettelijke taken van de afzonderlijke omgevingsdiensten?
- ...?

Mogelijkheden positionering:

- Data.OD wordt expliciet gepositioneerd als ontsluitingsvoorziening
- Data.Od wordt gepositioneerd als zelfstandig verwerkingsdoel onder de AVG

2. ROLVASTSTELLING



➤ **De rolvaststelling van Data.OD moet eenduidig en transparant beschreven zijn.**

Hierin moeten o.a. de volgende aspecten duidelijk naar voren komen:

- Zijn Omgevingsdiensten
 - Afzonderlijke verwerkingsverantwoordelijken, of
 - Gezamenlijke verwerkingsverantwoordelijken
- Wie is juridische eigenaar van het platform Data.OD

Dit moet worden vastgelegd via:

- Governance document
- Art. 26-overeenkomst (bij gezamenlijke verwerkingsverantwoordelijkheid)

UITLEG ROLVASTSTELLING

Niet het systeem is verantwoordelijk, maar de rol die men heeft onder de AVG. De AVG kent geen “technische eigenaar”, alleen juridische rollen. Kernvraag is wie verantwoordelijk is bij calamiteiten, zoals bv een hack.

Verwerkingsverantwoordelijke is de partij die:

- Het doel en het middel van de verwerking bepaalt
- Beslist welke data wordt verwerkt en waarom

De afzonderlijke OD's zijn verwerkingsverantwoordelijke voor hun eigen data (bv toezichtgegevens, vergunningen, handhavingsdata). Centralisatie verandert dit niet automatisch.

Gezamenlijke verwerkingsverantwoordelijken (art. 26 AVG) ontstaat als OD's:

- Gezamenlijk doelen en middelen vaststellen
- Gezamenlijk beslissen over gebruik van de data (bv. analyses over OD's heen)

Dan zijn de OD's gezamenlijk juridisch eigenaar. Zij moeten onderling vastleggen:

- Wie welk deel van de verantwoordelijkheid draagt
- Wie aanspreekpunt is voor betrokkenen
- Wie meldingen afhandelt

Zonder zo'n regeling zijn alle OD's volledig aansprakelijk.

3. VERWERKERSOVEREENKOMSTEN



➤ Stel (een) verwerkerovereenkomst(en) op voor Data.OD

Leg verwerkersovereenkomsten vast met:

- Data.OD beheerpartij
- Eventuele hostingpartij
- Leveranciers

Hierin staan expliciet:

- Beveiligingseisen
- Meldtermijnen
- Auditrechten

UITLEG VERWERKERSOVEREENKOMSTEN

Verwerker (art. 28 AVG) is de partij die:

- Data verwerkt in opdracht
- Zelf géén doel en/of middel bepaalt

Dit kan zijn:

- Een shared service organisatie
- Een IT-beheerpartij
- Een uitvoerende organisatie die Data.OD technisch beheert

4. KETENRISICO



➤ Beschrijf de ketenrisico's eenduidig en transparant

Implicaties die geregeld moeten zijn:

- Ketenafhankelijkheid en single point of failure;
- Eisen aan:
 - Netwerkbeveiliging;
 - Identity & access management (federatie, MFA, autorisaties);
 - Logging en monitoring over tenantgrenzen heen;
- Incident & response
 - Wie doet wat bij een datalek of security incident in Data.OD?

5. INCIDENT & RESPONSE

- **Beschrijf procedures rond incident & response bij calamiteiten (o.a. datalek, hack) zijn eenduidig en transparant**

Belangrijke aspecten hierbij:

- Wie detecteert
- Wie beslist
- Wie meldt
- Wie communiceert

Zonder dit uit te werken hebben we een bestuurlijk en juridisch risico.

UITLEG INCIDENT & RESPONSE

Wat gebeurt er concreet bij een hack/dataincident?

Stap 1 – Technische detectie & containment (Data.OD beheerorganisatie)

- Detecteert incident
- Sluit toegang af
- Stelt vast welke data geraakt is

Stap 2 – Juridische beoordeling (Verwerkingsverantwoordelijke(n))

- Beoordelen: is er sprake van een datalek onder de AVG?
- Bepalen risico voor betrokkenen

Stap 3 – Melding aan AP en betrokkenen

- Binnen 72 uur melding bij AP (indien risico)
- Eventueel melding aan burgers/bedrijven

Wie meldt?

- De (gezamenlijke) verwerkingsverantwoordelijke
- Vaak: één aangewezen OD namens de anderen

Verwerkers mogen dit niet zelfstandig doen, maar moeten wel onverwijld informeren.

UITLEG INCIDENT & RESPONSE

Wie is juridisch eigenaar en moet handelen?

De juridisch eigenaar is altijd één of meerdere OD's, nooit "Data.OD".

Rol	Bij hack verantwoordelijk voor
OD (individueel)	Eigen datasets
OD's gezamenlijk	Gedeelde / gezamenlijke datasets
Data.OD beheerder	Technische beveiliging & melding aan verwerkingsverantwoordelijke
Bestuur	Bestuurlijke verantwoordelijkheid
Functionaris gegevensbescherming	Onafhankelijk advies

6. BRONSPECIFIEKE AFSPRAKEN

- **Beschrijf per bron wat de specifieke afspraken zijn en leg privacy aspecten vast in het register van verwerking**

Leg per databron o.a. vast:

- Classificatie (minimaal open, intern, vertrouwelijk) van de bron
- Herkomst en wettelijke grondslag
- Hergebruik- en bewaartermijnen
- Wat zijn de leverancierseisen
 - Beschrijf mogelijke beperkingen
- Privacy aspecten
 - Welke persoonsgegevens zijn opgenomen in de dataset
 - Welke bijzondere persoonsgegevens zijn opgenomen in de dataset

UITLEG BRONSPECIFIEKE AFSPRAKEN

In de opzet van Data.OD wordt gesproken over

- Open data
- Gereguleerd datagebruik
- Privacygevoelige en minder privacygevoelige data

Dit vereist dat duidelijkheid wordt verschaft per aangesloten bron.

7. (PRÉ) DPIA

DPIA = Data Protecten Impact Assessment

- **Voer altijd een pré DPIA uit indien er persoonsgevoelige informatie wordt verwerkt binnen Data.OD**
 - Dit doen we per verwerking waarbij persoonsgevoelige informatie betrokken is
- **Wanneer de pré DPIA dit uitwijst moet altijd een DPIA uitgevoerd worden**

Zonder (pré) DPIA is centralisatie juridisch kwetsbaar

DPIA bij:

- Grootschalige monitoring
- Koppeling van OD-data
- Centrale analyse

Te regelen:

- Expliciet moment waarop privacy impact wordt getoetst;
- Koppeling tussen DPIA uitkomsten en ontwerpkeuzes.

8. GOVERNANCE

➤ Beschrijf de governance van Data.OD eenduidig en transparant

Belangrijke aspecten hierin:

- Wie is inhoudelijk verantwoordelijk voor Data.OD als platform?
- Waar is het beheer van Data.OD neergelegd?
 - Hoe is hierbij de continuïteit in beheer geborgd?
- Wie is per databron eigenaar, verantwoordelijke en beheerder?
- Waar liggen de rollen, taken en verantwoordelijkheden formeel vast?

Zonder expliciete rolafbakening ontstaat direct BIO non compliance (o.a. eigenaarschap, logging, incidentafhandeling).

Hoewel governance wordt benoemd, zien we in vergelijkbare trajecten vaak:

- Techniek en koppelingen lopen voor;
- Governance, mandaat en besluitvorming lopen achter.

Te beantwoorden / te regelen:

- Welke governance onderdelen zijn randvoorwaardelijk vóór productiegebruik?
- Welke onderdelen kunnen later volgen zonder risico voor rechtmatigheid en security?

9. OVERIGE SECURITY ASPECTEN

➤ **Geef inrichting aan overige belangrijke security aspecten en beschrijf dit eenduidig en transparant**

Belangrijke aspecten hierbij:

- Security & BIO
 - Welke BIO controls zijn expliciet van toepassing op Data.OD?
 - Hoe is logging, monitoring en incidentrespons ketenbreed ingericht?
 - Hoe is toegang geregeld (IAM, MFA, autorisatie per OD)?
- Architectuur & positie OD
 - Welke data wordt wel en niet lokaal opgeslagen bij OD's?
 - Hoe sluiten Data.OD koppelingen aan op de architectuurkaders van OD's?

10. OVERIGE PRIVACY ASPECTEN

➤ Geef inrichting aan overige belangrijke privacy aspecten en beschrijf dit eenduidig en transparant

Naast verantwoording over persoonsgevoelige informatie en het uitvoeren van een (pré) DPIA zijn de volgende privacy aspecten van essentieel belang:

- Technische maatregelen tegen function creep
- Dataminimalisatie bij ontsluiting (niet “alles ophalen omdat het kan”)
- Hoe is hergebruik en doorlevering beheerst

11. ARCHIVERING

➤ Geef inrichting aan archiveringsaspecten conform DUTO waar dit van toepassing is

In deze fase zullen de datasets “as is” van de externe bronnen afgenomen, verwerkt en aangeboden worden. De OD's en Data.OD in bijzonder hebben in deze dan ook geen archiveringsplicht. Wel zullen sets na de afgesproken bewaarperiode verwijderd moeten worden. Per dataleverantie wordt de bewaartermijn vastgesteld.

Data.OD

Het landelijke dataknooppunt voor
omgevingsdiensten in Nederland



DATA.OD



DCMR milieudienst
Rijnmond