

# Open up!

Gesprekken en reacties over 'pas toe of leg uit'-standaarden toepassen  
n.a.v. de Monitor Open Standaarden

Van: Bureau Forum Standaardisatie (Désirée Castillo Gosker en Ludwig Oberendorff)

Aan: Forum Standaardisatie (Larissa Zegveld, voorzitter)

Den Haag, 8 april 2021

## Inleiding

De onderzoekers van de Monitor Open Standaarden hebben in 2020 gesprekken gevoerd en gemaïld met ICT-inkopers/aanbestedingsprofessionals (vraagt u om de juiste open standaarden in een aanbesteding?) en met beheerders van diverse overheidsbrede voorzieningen (past u de relevante standaarden toe in de voorziening?). Deze gesprekken en contacten zijn verwerkt in drie verslagen, die aan de orde zijn gekomen in de Forumvergadering van 10 maart 2021 en waren op verschillende punten aanleiding tot een schrikreactie van Forumleden. Na 15 jaar "pas toe of leg uit"-beleid (b)lijken er nog diverse misverstanden te bestaan over de toepassing van de standaarden op de 'pas toe of leg uit'-lijst. Onder andere dat iedere organisatie alsnog zijn eigen risico afweging kan maken óf ze de standaarden gaat toepassen. En dat die "leg uit" niet op schrift in het jaarverslag hoeft, maar ook achteraf (uit het hoofd) kan worden geconstrueerd. Daarnaast vragen sommige overheidsorganisaties zich af, of ze überhaupt wel gebonden zijn door afspraken in het OBDO. Mede gelet op een aantal quotes van deze strekking wilde het Forum Standaardisatie graag een vervolg analyse; een notitie met conclusies op hoofdlijnen en actiepunten. Zie hier deze notitie. Daarin zijn enkele quotes uit de gespreksverslagen ter illustratie opgenomen.

Het is goed om te bedenken dat de input afkomstig is van twee heel verschillende groepen. Wat zij te zeggen hebben is heel divers maar er zijn ook overeenkomsten. Vijf punten komen bij beide groepen terug, die min of meer met elkaar samenhangen. In deze notitie staan deze punten, met daarbij reeds lopende acties die met het punt samenhangen en met suggesties voor acties voor de toekomst.

## Vraag aan het Forum

Het Forum Standaardisatie wordt gevraagd om de notitie te bespreken aan de hand van de volgende vragen:

1. Hoe kunnen besluiten op bestuursniveau over open standaarden beter en effectiever worden? Hoe kunnen ze meer en beter terecht komen op de werkvloer?
2. Er lopen verschillende acties vanuit het Forum, maar het is duidelijk dat meer actie van de organisaties zelf moet plaatsvinden. Hoe komen ze zover?

3. Kunt u aangeven of u het eens bent met de conclusies die hier getrokken worden en welke hier genoemde acties u het meest aanspreken?

Noot: Uw input wordt met name gevraagd t.a.v. voorgestelde acties die niet bij het Forum zelf liggen en eventuele andere suggesties voor acties van anderen. Dit met het oog op het vergroten van de cirkel van invloed.

## 5 punten

### 1. Top down besluiten laten landen

*"Het verbaasd ons dat u onze aanbesteding als slecht beoordeeld. Wij hebben voor de ontwikkeling van een app [...] een functionele specificatie opgesteld, waarbij wel geen enkele beperking hebben aangegeven met betrekking tot standaarden. Er kan natuurlijk gesteld worden dat wij niet specifiek gevraagd hebben om open standaarden, maar op deze manier hebben wij de markt in de gelegenheid gesteld om aan te bieden wat zij willen en kunnen. Er is voor hun dus alle vrijheid."*

Deze quote illustreert hoe het 'pas toe of leg uit'- beleid, in de vorm van besluiten op bestuursniveau in de praktijk vaak niet goed landt op de werkvloer bij hen die deze besluiten daadwerkelijk moeten uitvoeren.

Acties die lopen:

- Forum gaat langs in verschillende gremia (bestuurlijk, inkoop, informatiebeveiliging, CIO's, CTO's) bij verschillende overheidsdomeinen. Er wordt daarbij aangestuurd op een terugkomafpraak (herhaling loont, lange adem).
- Informatie uit IV-meting en Monitor Open Standaarden wordt zoveel mogelijk organisatiespecifiek gemaakt en geclusterd.
- Informatie uit IV-meting en Monitor Open Standaarden wordt zoveel mogelijk van onder naar boven opgewerkt: voorafstemming IV-meting via koepels (o.a. IBD, waterschappen, CIO-Rijk)

Acties ter overweging:

- Best practices in kaart brengen rondom
  - a) overheidsorganisaties waarin OBDO bestuurders informatie terugleggen in de organisatie & vervlechten in hun eigen kaders;
  - b) implementatietrajecten als domeinnaamregie (zoals VWS).
- Aansturen op het OBDO besluit, dat toepassen van "pas toe-of-leg-uit"-standaarden en de streefbeeldafspraken integraal onderdeel is van de taak van CIO-office & CIO oordelen. Dat eventueel opnemen in komende instellingsbesluit Forum en/of OBDO.
- Herhaling van het op organisatieniveau specifiek aanschrijven van overheidsorganisaties (zoals de briefmailing van zomer 2020).

### 2. Tell me why... overtuig me. Breng nut en noodzaak van het gebruik van open standaarden meer, en beter naar voren. Dat het verplicht is, is niet genoeg. Waarom is het gebruik van (deze) open standaarden belangrijk? Geef me zowel het grote plaatje als concrete voorbeelden.

*"Een standaard is een middel en geen doel. Voor het begrip en draagvlak moet je communiceren over het doel dat je ermee probeert te bereiken. Dat sneeuwt soms onder in de procedure. Ook in de rapportage*

*naar de kamer. Het zou mooi zijn als je meer op het doel en effect kan rapporteren. "*

Forum Standaardisatie worstelt al langer met deze communicatiekwesitie. Welk verhaal vertel je waar, wanneer is het te hoog over en te idealistisch (zie punt 1. knikt iedereen ja aan bestuurstafels en vervolgens gebeurt er weinig op de werkvloer) en wanneer is het te specifiek, te onnavolgbaar voor velen, te saai, te technisch, te diep in de uitvoering met te veel afkortingen? Wanneer moet je algemeen zijn, wanneer concreet. Hier is het niet *one size fits all* maar gaat het vaak om maatwerk.

### *Over broadcasting & narrowcasting*

Het juiste verhaal vertellen én inspirerend zijn én toegesneden op de doelgroep vormt de kern van ons werk en is continu in uitvoering. We praten niet voor niets zoveel. Het goede verhaal vertellen is maatwerk maar misschien biedt een vergelijking met de standaardconfectiematen XL t/m S toch wat verheldering.

### *Extra Large*

Het XL verhaal gaat over de rol van ICT en de rol van de overheid in de samenleving. Dit XL verhaal raakt aan een veel breder bewustwordingsproces en aan een veel grotere beleidsopdracht, die de opdracht van het Forum Standaardisatie ver overstijgt. Het Forum zou hier zeker een rol in kunnen spelen maar moet ook rolvast blijven.

### *Large*

Het Large verhaal gaat over hoe open standaarden horen bij de inrichting van een open samenleving. Met open standaarden vinden publieke waarden een technische vertaling in de digitale infrastructuur. In het algemeen dragen *open* standaarden bij aan ICT-kwaliteit, door interoperabiliteit en leveranciersonafhankelijkheid.

### *Medium*

Het Medium verhaal is meer afhankelijk van inhoud van de open standaard zelf. Hierover valt er een specifiek maar nog steeds vrij algemeen verhaal te vertellen. Over veiligheid en betrouwbaarheid (de informatieveiligheidsstandaarden) bijvoorbeeld, over inclusiviteit (denk aan de Digoegankelijkheid standaard), datakwaliteit en ketenverantwoordelijkheid. Ook hier in het kader van het hele publieke domein en niet alleen voor de overheid.

NB: Op het moment ligt er in de communicatie van het Forum Standaardisatie veel nadruk op gebruik van de informatieveiligheidsstandaarden op dit niveau. Misschien te veel maar dat is met reden. Inmiddels begrijpt een kritische massa door schade en schande wijzer geworden de urgentie van deze open standaarden en wij pakken deze golf. Door te hameren op het gebruik van deze standaarden en serieuswaargebeurde horrorverhalen te vertellen over spoofing, phishing en andere cybercriminaliteit die verschrikkelijk veel schade en geschaad vertrouwen veroorzaken. Gebruik deze informatieveiligheidsstandaarden en blijf gespaard, is de boodschap.

### *Small*

Het Small verhaal gaat over praktijkvoorbeelden. Welke organisaties gebruiken de standaarden, op welke manier, in samenwerking met welke andere organisaties, in welke informatieketen en hoe is de waarde die dat biedt merkbaar? De boodschap die loud en clear uit de gespreksverslagen blijkt: geef meer vooral meer verhalen op dit niveau.

### *Acties die lopen:*

- Video's maken over nut en noodzaak van het gebruik van open standaarden. In 2021 komt de eerste over de NL\_CIOUS standaard;

- In de Monitor Open Standaarden, wordt het onderdeel “overige gebruiksinformatie” meer kwalitatief dan kwantitatief ingericht en komt er meer aandacht voor nut en noodzaak van de standaarden op de ‘pas toe of leg uit’- lijst mét praktijkvoorbeelden;
- Organisaties die goed scoren in de Monitor Open Standaarden krijgen een eervolle vermelding op de website van Forum Standaardisatie en een oorkonde. We organiseren een webinar, in samenwerking met iBestuur; En als het allemaal weer kan, ook weer taart op kantoor;

### *Acties ter overweging*

- Voor het XL verhaal: Het Forum Standaardisatie zou de [Sustainable Development Goals](#) kunnen onderschrijven van de VN, ten einde een specifieke invulling te geven aan het begrip van duurzame ICT-kwaliteit. Dan kan aangesloten worden bij doelstellingen die o.a. gaan over innovatie (het creëren van een level playing field met open standaarden voor de markt), infrastructuur (de digitale infrastructuur is een vitale infrastructuur), inclusie (Digitoegankelijkheid), vrede, veiligheid en recht (informatieveiligheid) en een sterke publieke dienst (gezonde balans tussen het publieke en private domein).
- Een serie interviews houden. Kan ook in de vorm van video’s, of in de vorm van een podcast.

### **3. Are you a believer? De stille kracht van het individu. Aandacht voor open standaarden blijkt sterk afhankelijk van de overtuiging van individuen. Het onderwerp is nog nauwelijks geborgd in de structuur van organisaties en heeft veel concurrentie.**

“De adoptie en borging van open standaarden bij overheidsvoorzieningen hangt in grote mate af van de aandacht die er binnen een organisatie aan wordt besteed. Dat is vaak afhankelijk van individuele personen.”

“Vanzelfsprekend zullen wij zoveel mogelijk open standaarden uitvragen indien hier mogelijkheden voor zijn. Voornamelijk met SaaS applicaties (en daar gaat het hier om) moeten we toch voor een groot deel schikken naar hetgeen de leverancier maakt en verkoopt. Dit zijn over het algemeen geen openstandaard software pakketten. Het eisen van een totale open standaard, SaaS applicatie zal ervoor zorgdragen dat de meest belangrijke partijen met de gewenste functionaliteiten niet gaan inschrijven.”

Zoals gezegd laten de resultaten van de Monitor Open Standaarden en de IV-metingen een gat zien tussen wat op bestuursniveau besloten wordt en wat er in de praktijk gebeurt. “Pas toe of leg uit” wordt niet altijd begrepen als een verplichting of een dringend advies maar regelmatig als een “wist je dat je” zonder consequenties. Het is opvallend dat als het goed gaat, dit vaak komt door geïnspireerde individuen. Zij krijgen vaak veel voor elkaar maar geven ook aan structurele inbedding in hun organisatie te missen.

#### *Acties die lopen:*

- Forum en OBDO leden vragen om Monitor en de IV-meting te agenderen in hun achterban;
- Diverse bestuurlijke gremia aflopen met Monitor en de IV-meting;
- Verkenning van BZK hoe open standaarden meer en beter vervlochten kunnen worden in reeds bestaande kaders;
- Knelpuntenonderzoek dat is toegezegd aan de Tweede Kamer.

#### *Actie ter overweging:*

- Per organisatie op de juiste afdeling een ambassadeur met een opdracht voor open standaarden van de ‘pas toe of leg uit’- lijst instellen. Ook als aanspreekpunt voor de Monitor.

- Er wordt een modulaire tekst opgesteld over
  - a) het waarom van informatieveiligheid standaarden en de samenhang met trajecten als BIO, basis op orde en domeinnaambeheer;
  - b) daarbij wordt een FAQ gemaakt over o.a. de ptolu verplichting (o.a. geen eigen risico assessment; term 'uiterlijk' betekent dan klaar ipv. dan startdatum) en de verhouding met de streefbeeldafspraken en de WDO. Deze modulaire teksten kunnen dan als bouwblokken gebruikt worden binnen de verschillende domeinen.

#### 4. Meten is prikken en praten.

*"De monitor open standaarden helpt bij het geven van opdrachten om implementatie van standaarden intern te verbeteren."*

De jaarlijkse Monitor Open Standaarden en de halfjaarlijkse IV-metingen helpen om het onderwerp levend te houden in organisaties. Ook zeggen mensen behoefte te hebben aan dashboard. Het onderzoek uitvoeren is zélf ook een adoptieactiviteit en het is er een die werkt. Dat mensen zeggen behoefte te hebben aan een dashboard interpreteer ik als een behoefte aan meer zelfstandige spiegeling en interactie.

##### *Acties die lopen:*

- BFS heeft afgesproken om met ICTU na te denken hoe de Monitor Open Standaarden interactiever kan;
- BFS wil meer doen met de onderzoeksresultaten op de website van het Forum Standaardisatie.

##### *Actie ter overweging*

- Verkennen of het zin heeft om aan te sluiten bij reeds bestaande dashboards, zoals bijvoorbeeld voor Maatschappelijk verantwoord inkopen.

#### 5. Leg uit is dood, leve het gesprek!

*"Het fenomeen 'leg uit' leeft totaal niet bij bestuurders. Dat is wel een noodzakelijke voorwaarde om zaken op dit punt in beweging te krijgen."*

*"De projectleider die deze aanbesteding heeft gecoördineerd en ook de stukken heeft geschreven is inmiddels niet meer bij ons werkzaam. Zelf ben ik maar zijdelings betrokken geweest. Wij kunnen u dan ook helaas niet de verzochte informatie aanleveren."*

Uit de Monitor Open Standaardisatie blijkt al jaren dat het "leg uit" gedeelte van de "pas toe of leg uit" verplichting niet wordt nageleefd zoals de bedoeling is. Namelijk in het jaarverslag en met een geldige reden. Een geldige reden kan zijn omdat de standaard onvoldoende wordt ondersteund door de markt, onvoldoende veilig blijkt te zijn of een andere reden van bijzonder gewicht.

Deze officiële weg lijkt voorsnog een doodlopende weg. Dat komt onder meer omdat de naleving van de Rijksinstructie niet gehandhaafd wordt. Verder werkt het "leg uit" deel niet, als het erom gaat te achterhalen waarom het gebruik van standaarden achterwege wordt gelaten. Daarom wordt rond de Monitor consequent ingezet op gesprekken met overheidsorganisaties over projecten waar het goed is gegaan, en waar het minder goed is gegaan. Opvallend is dat daar zelden standaard-inhoudelijke leg-uit redenen naar voren komen om een standaard niet toe te passen. Of een risico-assessment rond de invoering van de specifieke standaard, die er toe leidt de standaard niet toe te passen. Veeleer wordt aangevoerd dat hun leverancier de standaard niet ondersteund, of dat er andere prioriteiten zijn.

### *Acties die lopen:*

- BZK/DO is in gesprek met de Audit Dienst Rijk. Handhaving van de Pas-toe-of-leg-uit Rijksinstructie heeft geen prioriteit in de wettelijke taak van de ADR. De ADR is gevraagd aandacht te vragen voor de Rijksbegrotingsvoorschriften op dit punt, bij de aanschrijving voor de jaar verantwoording;
- BZK/DO is in gesprek geweest met Financiën over aanscherping van de Rijksbegrotingsvoorschriften op het punt van "leg uit";

### *Actie ter overweging*

- Vanuit BZK/DO vraaggestuurde opdracht aan ADR en/of Rekenkamer geven t.a.v. zowel "pas toe" als "leg uit".

### **Tot slot**

Ik wil hier van de gelegenheid gebruik maken om de onderzoekers van de Monitor Open Standaarden te bedanken en een ieder die met hen van gedachten heeft gewisseld. Bedankt voor het voeren van het gesprek en de openheid.