

Tweede Nota van inlichtingen

Betreft	Tweede Nota van Inlichtingen	Datum	09-02-2023
Van	SPPOH	Ref.	KQPN/2023/10
Project	Europese aanbesteding ondersteuningsapplicatie		

Deze nota van inlichtingen wordt hiermee integraal onderdeel van het beschrijvend document. In geval van tegenstrijdigheden tussen de nota van inlichtingen en het beschrijvend document prevaleert het bepaalde in de nota van inlichtingen. Indien er meer nota's van inlichtingen zijn prevaleert, in geval van tegenstrijdigheden tussen de nota's van inlichtingen, het bepaalde in de meest recente nota van inlichtingen, dus die met het hoogste nummer.

Nr.	Betreft (pag. par. Overige verwijzing)	Vraag
1.	Aanbestedingsleidraad § 6, Algemeen	In de huidige applicatie zit een koppeling met de regionale Scholenwijzer, om de NAW gegevens van scholen uit op te halen en mee te synchroniseren. Deze wens staat niet in het huidige programma van eisen. Komt deze koppeling daarmee te vervallen?
Antwoord	Aanbestedingsleidraad 6.3 heeft als eis 11 het volgende opgenomen: Mogelijkheid tot het uniek opvoeren van leerlingen en koppelen aan gangbare Leerling Administratie systemen, tenminste ESIS, OSO en Parnasys met NAW, telefoon, email en BSN-nummer door gebruikers. Het is voor SPPOH niet van belang of dit via een koppeling of via een andere weg voldaan wordt aan deze eis. Een koppeling geniet de voorkeur.	

Nr.	betreft	Vraag
2.	Aanbestedingsleidraad § 6.3, Eis 28	Tot nu toe staat DUO niet toe dat er een koppeling gemaakt wordt met het Verzuimregister indien de koppelende partij geen school is. Het SWV mag wettelijk geen inzage hebben in het Verzuimregister. Deze eis is o.i. daarmee wettelijk niet te vervullen. a. Is de aanbestedende dienst bereidt deze eis te laten vervallen indien wettelijk niet gekoppeld mag worden?

		b. Zo nee, hoe ziet de aanbestedende dienst deze eis gerealiseerd worden?
Antwoord	Eis 28 vervalt.	

Nr.	Betreft (pag. par. Overige verwijzing)	Vraag
3.	Aanbestedingsleidraad § 6.5	Deze paragraaf gaat over Centraal Aanmelden SO/SBO. Door het opnemen van deze informatie als onderdeel van het Programma van Eisen wekt u de indruk dat deze functionaliteit qua ontwikkeling en kosten in de aanbestedingsprijs inbegrepen moet zijn. Valt de ontwikkeling en licentieprij van bovenstaande functionaliteit binnen de in te vullen prijs op bijlage 7 Prijzenblad?
Antwoord	Nee	

Nr.	betreft	Vraag
4.	Aanbestedingsleidraad § 6.7, Eis 2	Voor het realiseren van een generiek koppelvak is de medewerking van de leverancier nodig waarmee gekoppeld dient te worden. De ervaring leert dat niet iedere leverancier hiervoor open staat. Is de aanbestedende dienst bereidt deze eis te laten vervallen bij uitblijven van medewerking door de andere leverancier?
Antwoord	Het bereiken van samenwerking met de leverancier voor de realisatie van een generiek koppelvak is een verantwoordelijkheid van SPPOH. Indien die samenwerking tot stand komt, moet opdrachtnemer dit generieke koppelvak realiseren.	

Nr.	betreft	Vraag
5.	Aanbestedingsleidraad § 6.7, Eis 11	Wat is, naast de disproportionaliteit van deze eis, de motivatie om de eis te stellen dat inschrijver beschikt over een ISAE3402 rapportage? a. Kunt u duidelijkheid geven over de reden om deze eis te stellen. Wat is - in de lijn van het advies van de Commissie van Aanbestedingsexperts - de onderbouwing voor de Aanbestedende Dienst deze rapportage te eisen?

		b. Waarom stelt Aanbestedende Dienst de eis voor een ISAE-rapportage, omdat de inschrijver niet verantwoordelijk is voor het inhoudelijk beheer van de applicatie maar de Aanbestedende Dienst zelf? De correctheid en werking van de applicaties is immers afhankelijk van het gebruik van de applicatie door Aanbestedende Dienst zelf. c. Kan Aanbestedende Dienst uitleggen waarom de eis van een ISAE 3402 rapportage wordt gesteld terwijl deze eis elders in het onderwijs niet wordt gesteld (het Certificeringsschema is gebruikelijk)?
Antwoord	Aanbestedende Dienst acht deze eis niet disproportioneel. a. Aanbestedende Dienst wil zien dat Inschrijver in control is, en de externe accountant van Aanbestedende Dienst zal de risico's van het uitbestede proces willen kunnen beoordelen bij het opstellen van de jaarrekening. In het proces/de applicatie worden gegevens over (verantwoording van) gelden verwerkt. Inschrijver stelt de applicatie ter ondersteuning van dat proces beschikbaar en beheert de applicatie. b. In het rapport kan in de doelstelling en scope bv. aangegeven worden dat dienstverlening zich beperkt tot systeem-, en applicatiebeheer, beveiliging en monitoring. c. ISAE 3402 rapporten worden - met name door uitbesteding van processen via SaaS-applicaties waarin transacties worden gedaan voor geldstromen of bekostiging - in toenemende mate vereist door accountants, zo ook in de onderwijssector. Daarbij geldt dat steeds meer dienstverleners in het onderwijs dergelijke rapportages leveren (zie bijvoorbeeld Iddink Digital BV voor hun leerling-administratiesysteem Magister).	

Nr.	betreft	Vraag
6.	Aanbestedingsleidraad § 6.8, Eis 1	De NEN7510 is niet gelijkwaardig aan de ISO27001, toch doet de Aanbestedende Dienst het voorkomen dat deze eisen gelijkwaardig zijn door de term 'en/of'. Verder is de NEN7510 een norm die in de zorg wordt gehanteerd en in het onderwijs niet gehanteerd wordt en niet relevant is. a. Op basis waarvan meent de Aanbestedende Dienst dat de ISO en NEN norm van eis 1 gelijkwaardig zijn? b. Waarom meent Aanbestedende Dienst dat het stellen van de eis om een NEN7510-certificaat voor het onderwijs relevant en afdoende is om daarmee aan te tonen dat informatiebeveiliging geregeld is? c. Kan de Aanbestedende Dienst uitleggen waarom de eis van de NEN7510, die afwijkt van wat in de onderwijssector

		gebruikelijk is, in deze aanbesteding een relevante eis is om te stellen?
Antwoord	a. De Nederlandse NEN7510-norm is grotendeels gebaseerd op ISO27001 (en ISO27002). Ondanks de verschillen (o.a. ook de extra normen die NEN7510 kent) acht de Aanbestedende Dienst de NEN7510-norm geschikt (zie ook b en c). b. Omdat dit ook zo werkt voor de zorgsector, waarin vanwege de vele bijzondere persoonsgegevens de normen zeker niet minder streng zijn dan in het onderwijs. c. Omdat Aanbestedende Dienst in het kader van passend onderwijs met name gezondheidsgegevens verwerkt; daarmee zijn risico's overeenkomstig de zorgsector.	

Nr.	betreft	Vraag
7.	Aanbestedingsleidraad § 6.7, Eis 11, § 6.8, Eis 1 en 6.	Inschrijver onderschrijft de wens van Aanbestedende Dienst dat de persoonsgegevens van leerlingen, ouders en medewerkers goed beschermd zijn. De wijze hoe Aanbestedende Dienst daar invulling aan geeft, is o.i. echter niet helder en transparant en buitenproportioneel. We vragen ons af hoe de eis voor een ISO27001 en/of NEN7510-certificaat zich verhoudt tot eis 5 (voldoen aan art 32 AVG), eis 6 (hanteren Certificeringsschema) en § 6.7 eis 11 (ISAE 3402 rapportage)? Aanbestedende Dienst legt inschrijvers meerdere eisen op die o.i. overlappen of net verschillen. Artikel 32 AVG (eis 5) is de wettelijke verplichting om persoonsgegevens te beveiligen, en volgens de visie van de Autoriteit Persoonsgegevens is - bij gebreke van een sectorale invulling van een beveiligingsnorm - de ISO 27001 de norm voor beveiligen van persoonsgegevens. Eis 6 betreft het Certificeringsschema, wat binnen de onderwijssector de sectorale invulling is, waar de AP over spreekt. Een sectorale invulling ontbreekt hier dus niet. Het certificeringsschema gaat weliswaar uit van de ISO27001, maar wijkt op een aantal onderdelen af van de ISO27001. Eis 11 uit § 6.7 wijkt weer af van wat door de Autoriteit Persoonsgegevens als eis wordt gesteld aan verwerken van persoonsgegevens, terwijl Aanbestedende Dienst deze eis wel aan de inschrijver oplegt. a. We gaan ervan uit dat de aanbestedende dienst de volgende interpretatie bedoeld bij bovenstaande eisen: “Aanbestedende Dienst ziet de eisen wel als complementair. Eis 5 zou dan het wettelijke kader

		zijn in verband met privacy. In Eis 1 wordt dan verwezen naar een algemene en internationale norm voor informatiebeveiliging (en niet alleen privacy) die onafhankelijk wordt getoetst en daarmee aantoonbaar is. Eis 5 verwijst dan ‘alleen’ naar het praktische toetsingskader met maatregelen (gebaseerd op ISO27001) behorende bij het op onderwijs gerichte ROSA- certificeringsschema. Deze eis betreft daarmee niet het gehele ROSA- certificeringsschema. Eis 15 betreft een rapportage die is opgesteld door een onafhankelijke, gecertificeerde auditor of accountant met financiële processen/procedures als voornaamste reikwijdte.” Klopt deze interpretatie? Zo nee, kunt u uw interpretatie van deze ogenschijnlijk overlappende eisen uiteen zetten? b. Heeft de inschrijver de keuze om te kiezen tussen: - ISO 27001 in combinatie met het praktisch toetsingskader behorend bij het ROSA certificeringsschema; - of - Het gehele ROSA-certificeringsschema (als goede norm voor het onderwijs) te hanteren. Indien dit niet de keuzes zijn, kan de aanbestedende dienst dan uiteenzetten op welke onderdelen inschrijver moet voldoen aan ISO27001, en op welke punten aan het Certificeringsschema? c. Hoe verhoudt het stellen van eis 6 zich tot eis 1 (ISO27001/NEN7510) en eis 11 § 6.7 (ISAE3402), aangezien de Autoriteit Persoonsgegevens uitgaat van de norm voor informatiebeveiliging die in een sector wordt gehanteerd (voor het onderwijs is dat het Certificeringsschema) en bij gebreke daarvan aan de ISO27001.
Antwoord	a. Deze interpretatie klopt. b. Ja, Inschrijver kan tussen de gestelde opties kiezen. c. Dat de AP dit formeel als standpunt heeft, is Aanbestedende Dienst onbekend. Aanbestedende Dienst hanteert hetzelfde standpunt als het Privacyconvenant (PC) Onderwijs (zie bijvoorbeeld Toelichting bij de vereisten voor Bijlage 2, p11).	

Nr.	betreft	Vraag
-----	---------	-------

8.	Aanbestedingsleidraad § 6.8, Eis 4	Wij hanteren voor ons platform en alle modules de BIV classificatie 3, 2, 3. Kan u hiermee akkoord gaan? Ingeval de aanbestedende dienst niet akkoord gaat: kan de aanbestedende dienst aangeven waarom er tot nu toe gebruik is gemaakt van een applicatie die deze classificatie wel hanteert en dit wel geaccepteerd werd?
Antwoord	Akkoord	

Nr.	betreft	Vraag
9.	Aanbestedingsleidraad § 6.8, Eis 17	Volgens artikel 7 lid 2 van het privacyconvenant, moeten betrokkenen zich richten tot de Aanbestedende Dienst als het gaat om het uitoefenen van de rechten van betrokkenen. Het wordt verwerkers, zoals inschrijvers, verboden om zich daarmee bezig te houden en zij moeten betrokkenen (ouders, leerlingen, medewerkers) verwijzen naar de school, bestuur of samenwerkingsverband. a. Wat bedoelt Aanbestedende Dienst, in het licht van de verplichtingen uit de AVG en de formuleringen in het privacy- convenant, met "standaard informatie en procedures" waar inschrijver over moet beschikken? b. Moet inschrijver beschikken over procedures om verzoeken van betrokkenen met betrekking tot het uitoefenen van hun rechten, te verwijzen naar de Aanbestedende Dienst? c. Hoe ziet de Aanbestedende Dienst "de standaard informatie" waar inschrijver over zou moeten beschikken, nu het de verplichting is van Aanbestedende Dienst om betrokkenen deze informatie te verschaffen?
Antwoord	a. Inschrijver dient (conform AVG art. 28 lid 3e en 3g, maar ook conform PC Model Verwerkersovereenkomst Digitale onderwijsmiddelen en privacy 4.0 - 2022 art. 9 lid 1a) bijstand te verlenen in de vorm van informatie en procedures bij het doen nakomen van de op Aanbestedende Dienst rustende verplichtingen op grond van de AVG met betrekking tot de in hoofdstuk III van de AVG vastgelegde rechten van de betrokkene(n) binnen de wettelijke termijnen, zoals bij een verzoek om inzage of een kopie, verwijdering, afscherming of overdraagbaarheid van persoonsgegevens. b. Ja. c. Nader te bepalen, maar bijvoorbeeld in de vorm van rapportages/logboeken/ handleidingen en dus niet met de Betrokkene(n) als doelgroep, maar de Aanbestedende Dienst als doelgroep om te kunnen voldoen aan de verplichtingen.	

Nr.	betreft	Vraag
-----	---------	-------

10.	Aanbestedingsleidraad § 6.8, Eis 18	De Aanbestedende Dienst stelt de eis om data exportabel te laten zijn in het kader van de rechten van betrokkenen. Inschrijver snapt niet waarom deze eis wordt gesteld. Volgens artikel 20 AVG geldt het recht op dataportabiliteit niet voor Aanbestedende Dienst, omdat er géén sprake is van persoonsgegevens van leerlingen en hun ouders die met hun toestemming worden verwerkt, of op de grondslag overeenkomst worden verwerkt. De informatie die in de systemen van inschrijver komen, vallen onder de in de AVG opgenomen grondslag wettelijke verplichting, taak van algemeen belang of openbaar gezag of gerechtvaardigd belang. a. Kan Aanbestedende Dienst een toelichting geven waarom Inschrijver dan toch aan dataportabiliteit moet voldoen? b. Bedoeld de Aanbestedende Dienst hier dat bij een overstap naar een andere leverancier de data eenvoudig te migreren moet zijn?
Antwoord	a. Hoewel beperkt is het wel degelijk zo dat ook persoonsgegevens (kunnen) worden verwerkt op basis van toestemming of op basis van een overeenkomst. b. Nee, dat geldt ook maar staat hier los van. Hier wordt het recht op overdraagbaarheid bedoeld zoals gesteld in AVG art. 20. Betrokkenen moeten de persoonsgegevens die ze (rekening houdend met de grondslagen zoals benoemd in a) aan Aanbestedende Dienst hebben verstrekt, in een gestructureerd, gangbaar en machineleesbaar formaat kunnen ontvangen en deze aan een andere Verwerkingsverantwoordelijke kunnen overdragen.	

Nr.	betreft	Vraag
11.	Aanbestedingsleidraad § 6.8, Eis 19	Uw minimale eisen rondom wachtwoordbeheer zijn bijzonder specifiek. O.i. mag van een inschrijver die een standaard oplossing dient te bieden, zoals beschreven in uw eisen, worden verwacht dat er aan een degelijke wachtwoordbeleid is. Eén die voldoet aan gangbare standaarden, zoals ook vanuit het Certificeringsschema vereist is. a. Waarom kiest de aanbestedende dienst ervoor om hier op de stoel van de inschrijver te gaan zitten en deze hele specifieke eisen te stellen, die waarschijnlijk maatwerk vereisen, iets wat volgens u zoveel mogelijk vermeden moet worden? b. Zijn de eisen van het wachtwoord/zin-beleid gebaseerd op een éénduidige (inter)nationale standaard of richtlijn, en/of een door de overheid gehanteerde norm? c. Zo ja, welke?

		d. Bent u bereid om zich te conformeren aan een erkende richtlijn omtrent deze eis zoals al toegepast door inschrijver, om mede hiermee maatwerk en aanvullende kosten te voorkomen ?
Antwoord	a. SPPOH heeft niet de ambitie om op de stoel van de inschrijver te gaan zitten. b. Ja, deels c. Gebaseerd op NIST (zie: https://pages.nist.gov/800-63-3/) en vanuit daar vertaald naar een praktische, passende uitwerking (mede gevoed door onder andere www.veiliginternetten.nl). d. Nvt, maar indien Inschrijver een betere standaard of richtlijn voorstelt inclusief praktische, passende uitwerking dan wil Aanbestedende dienst het overwegen.	

Nr.	betreft	Vraag
12.	Aanbestedingsleidraad § 6.9, Eis 9	Onze ServiceDesk is ma. t/m do. telefonisch bereikbaar van 9.00 tot 12.30 en van 13.00 tot 17.00 en op vrij. van 9.00 tot 12.30. Binnen reguliere kantooruren (9.00 tot 17.00 uur) is de SD ook altijd bereikbaar via mail. Dit aanpassen voor 1 klant vraagt o.i. buitensporige en kostbare aanpassingen in onze organisatie en is voor ons daarmee niet in lijn met de eerdere opmerking van de aanbestedende dienst dat er zo min mogelijk maatwerk moet worden geleverd. Gaat de aanbestedende dienst akkoord met deze bereikbaarheid?
Antwoord	Nee, deze eis blijft gehandhaafd.	

Nr.	betreft	Vraag
13.	Aanbestedingsleidraad § 6.9, Eis 13 en 15	U stelt dat de oplostijd bij storingen maximaal 8 werkuren dient te zijn. Gezien de interpretatiemogelijkheid van uw eisen is er een aparte SLA nodig met de aanbestedende dienst die af zal gaan wijken van onze standaard SLA. U stelt echter ook dat maatwerk zoveel mogelijk vermeden moet worden. Los de aanvullende kosten die een maatwerk SLA met zich meebrengt in de totaalprijs van een project, is het gebruikelijk om verschillende categoriegroepen te definiëren voor incidenten/storingen. Dergelijk prioritering geeft ruimte voor verschillende afhandelings tijden, zodat kosten proportioneel blijven. Deze differentiatie mist nu in uw eis. De kosten voor een SLA waarbij alle storingen dezelfde

		prioriteit en maximale oplostijd hebben, zijn buitenproportioneel hoog en onnodig in onze optiek. a. Onderschrijft u bovenstaande stellingen? b. Zo ja, kunt u een beschrijving of definitie geven van de verschillende categorieën die u wenst te hanteren, met bijbehorende beschrijvingen en gewenste oplostijden? Indien dit niet mogelijk is, hoe wenst u hier dan mee om te gaan? c. Kunt u akkoord gaan met de standaard SLA van inschrijver?
Antwoord	a. Nee b. NVT c. Nee	

Nr.	betreft	Vraag
14.	Inkoopvoorwaarden art 7.6	Dit artikel lijkt te beschrijven dat SPPOH in alle gevallen onder een gehele contractuele verplichting uit kan, indien SPPOH zelf om een aanpassing of aanvulling van de opdracht vraagt en deze bij ontvangen van de prijsopgave, de aanpassing of aanvulling te duur vindt. O.i. kan dit niet de bedoeling zijn van de aanbestedende dienst bij dit artikel. Wij kunnen het echter niet anders interpreteren. Het lijkt ons juridisch ook niet houdbaar. Wat zijn de eigenlijke intenties achter, en de juist interpretatie van dit artikel?
Antwoord	Artikel 7.6 van de inkoopvoorwaarden vervalt.	

Nr.	betreft	Vraag
15.	Inkoopvoorwaarden art 10.3	Hier wordt gesteld dat de kosten voor inspecties of keuringen die SPPOH initieert, altijd gedragen worden door de opdrachtnemer. Dit zou betekenen dat de aanbestedende dienst 4 keer per maand testen kan initiëren, waar opdrachtnemer dan voor moet betalen. Dit is onacceptabel voor inschrijver. Gebruikelijk is dat de opdrachtgever zelf de kosten draagt voor zelf geïnitieerde keuringen en inspecties. Verder is het gebruikelijk om afspraken te maken op voorhand over welke inspecties plaats gaan vinden en hoe frequent dit zal gebeuren, zodat opdrachtnemer dit kan begroten en eventueel kan meecalculeren in de aanbieding.

		a. Is hier sprake van een typefout en wordt er opdrachtgever bedoeld? b. Zo nee, is de aanbestedende dienst bereidt dit artikel zodanig aan te passen dat er redelijkheid en grip voor opdrachtgever en opdrachtnemer op de hiermee gepaard gaande kosten ontstaat? B.v. tijdens een verificatiegesprek?
Antwoord	A. Nee B. Inspecties en/of keuringen zullen niet op reguliere basis worden uitgevoerd. Indien Opdrachtgever een inspectie of keuring wil laten uitvoeren of zelf uitvoert, worden die kosten gedragen door Opdrachtgever.	

Nr.	betreft	Vraag
16.	Inkoopvoorwaarden art 22.1 c	Het feit dat het contract geheel of gedeeltelijk ontbonden kan worden bij een directie- of aandeelhouderswissel van opdrachtnemer is niet acceptabel voor inschrijver. a. Is aanbestedende dienst bereidt dit artikel te laten vervallen? b. Zo nee, kan de aanbestedende dienst aangeven wat de achterliggende gedachte is om deze voorwaarde op te nemen en beschrijven wat de aanbestedende dienst aan andere voorwaarden of zekerheden zou accepteren om dit artikel niet toe te passen bij een directie- of aandeelhouderswissel?
Antwoord	a. Ja b. NVT.	