2e Nota van inlichtingen: Advisering, ondersteuning en uitvoering op het gebied van Security diensten

Participatiefonds

Datum: 2-2-2023

Mededeling Aanbestedende dienst:

Naar aanleiding van vraag 1 en 2 in de 2e Nota van inlichtingen: Advisering, ondersteuning en uitvoering op het gebied van Security diensten heeft de Aanbestedende dienst het volgende besloten:

De geschiktheidseisen m.b.t. hoofdstuk 3.2.3.1. Kerncompetenties zijn aangepast, zie hiervoor de beantwoording van vraag 1 en 2 van de 2e Nota van inlichtingen: Advisering, ondersteuning en uitvoering op het gebied van Security diensten.

Dit resulteert in een rectificatie van de Kerncompetenties, waardoor de Aanbestedende dienst de planning heeft aangepast. Een 3e Nota van inlichtingen wordt beschikbaar gesteld en de uiterlijke ontvangst van inschrijvingen is verplaatst, zie hiervoor de rectificatie in Tenderned.

Nr	Categorie	Betreft	Gestelde vraag	Antwoord
1	Proces	Eerste NvI vraag 31:	In uw antwoord geeft u aan dat Inschrijver een vergelijkbare opdracht (advisering, ondersteuning en uitvoering op het gebied van Security diensten) per thema te hebben uitgevoerd met een minimale totale opdrachtwaarde (alle thema's bij elkaar) van € 350.000,- excl. BTW. Kunt u instemmen met een referentie voor een vergelijkbare opdracht per thema en als zodanig (maximaal) vier referenties die het totaal van de opdrachtwaarde omvat?	Ja, wij kunnen er (alsnog) mee instemmen, dat de met kerncompetentie 1 gevraagde ervaring ook kan worden aangetoond met maximaal vier (4) referte-opdrachten per thema afzonderlijk die tezamen een waarde vertegenwoordigen van tenminste € 350.000,- excl. BTW.
2	Proces	Eerste NvI vraag 30:	In uw antwoord geeft u aan dat het aantal drie per abuis is vermeld en dat u verwacht dat de Inschrijver een vergelijkbare opdracht (advisering, ondersteuning en uitvoering op het gebied van Security diensten) binnen een (semi-)overheidsorganisatie met minimaal 60 FTE's heeft uitgevoerd. Kunt u instemmen met een referentie voor een vergelijkbare opdracht per thema en als zodanig (maximaal) vier referenties? En kunt u instemmen met een referentie bij een andersoortige organisatie dan (semi-)overheid, wanneer deze het gevraagde per thema vertegenwoordigd?	1. Nee, de eis 'minimaal 60 FTE's' bij kerncompetentie 2 blijft staan. Wij willen immers een bepaalde omvang bij een eerder uitgevoerde (vergelijkbare) referteopdracht zien. 2. Wij stemmen wel in met het loslaten van de minimumeis 'binnen een (semi-)overheidsorganisatie'.
3	Juridisch	Eerste NvI vraag 25	In uw antwoord geeft u aan dat opdrachtnemer in het kader van dit contract zelfstandig verwerkingsverantwoordelijke is. U geeft daarnaast aan dat indien er sprake zou zijn van het beoordelen en testen van infrastructuur en maatregelen waarbij gebruik wordt gemaakt van persoonsgegevens er wel sprake is van werkgeverschap. Wij hebben twee vragen over dit statement: • Het beoordelen en testen van infrastructuur en maatregelen waarbij gebruik wordt gemaakt van persoonsgegevens is dus geen onderdeel van de huidige uitvraag? • Wij zijn van mening dat ook bij deze werkzaamheden opdrachtnemer in beginsel als zelfstandig verwerkingsverantwoordelijke kwalificeert. De opdracht is in dat kader namelijk het beoordelen en testen van infrastructuur en maatregelen en niet primair het verwerken van persoonsgegevens. Dat er bij het beoordelen en testen persoonsgegevens verwerkt dienen te worden is een uitvloeisel van de dienstverlening. Bij eis 15 uit het PvE staat het woordje 'en'. Het dient dus te gaan om namelijk het beoordelen en testen van infrastructuur en maatregelen en een opdracht die specifiek gericht is op het verwerken van persoonsgegevens. Dat laatste zal echter niet vaak aan de orde zijn gezien de inhoud van dergelijke opdrachten. Wij willen u derhalve vragen om te bevestigingen dat Opdrachtnemer bij een dergelijke opdracht niet per definitie aangemerkt wordt als verwerker maar dat partijen kijken naar de specifieke aard van de dienstverlening en de feitelijke invulling daarvan om te bepaling of opdrachtnemer als verwerker of als verwerkingsverantwoordelijke kwalificeert. Kunt u hiermee instemmen?	De eerste vraag is niet op voorhand te beantwoorden. De opdracht ziet in de basis niet op het verwerken van persoonsgegevens. Als er in dit traject zich onverhoopt de situatie voordoet dat dit wel het geval gaat zijn, dus de opdracht richt zich primair op het verwerken van persoonsgegevens, dan wordt een verwerkersovereenkomst afgesloten. Op voorhand valt dus geen uitsluitsel te geven op de eerste vraag. Opdrachtgever herhaalt het standpunt - gesteund door de EDPB, AP en de Handleiding AVG (Ministerie van J&V) - dat zodra opdrachtnemer werkzaamheden gaat uitvoeren die primair gericht zijn op het verwerken van persoonsgegevens opdrachtgever verwerkingsverantwoordelijke is en opdrachtnemer verwerker. Een verwerkersovereenkomst wordt in dat geval gesloten.

4	Juridisch	Eerste NvI vraag 23:	U geeft aan dat u de door ons voorgestelde tekst niet wilt overnemen omdat hiermee de onderzoeksplicht van opdrachtnemer zinledig wordt gemaakt. U bent het er echter wel mee eens dat Opdrachtgever verantwoordelijk is voor de juistheid, volledigheid en betrouwbaarheid door hem verstrekte informatie. Met de voorgestelde tekst wensen wij echter het uitgangspunt vast te leggen; opdrachtnemer mag uitgaan van de juistheid, volledigheid en betrouwbaarheid van de aan haar verstrekte informatie. Opdrachtnemer voert immers geen audit uit op de juistheid van de aan haar verstrekte informatie, dat betreft ook geen onderdeel van de opdracht. Uiteraard hebben wij zelf ook een verplichting omtrent de verkregen informatie, het is niet de bedoeling om deze buiten werking te stellen. Om dit weer te geven willen wij u vragen om in te stemmen met de toevoeging van de volgende tekst: "4.5 Opdrachtnemer mag uitgaan van de juistheid, volledigheid en betrouwbaarheid van de aan Opdrachtnemer verstrekte informatie, ook indien deze van derden afkomstig is tenzij Opdrachtnemer weet of redelijkerwijs behoort te weten dat de verkregen informatie onjuist, onvolledig of onbetrouwbaar is."	Wij stemmen daar niet mee in. Wij zijn (echter) wel bereid om navolgend nieuw artikellid 4.5 aan artikel 4 ARBIT-2022 toe te voegen: "4.5 wederpartij mag uitgaan van de juistheid van de door opdrachtgever aan wederpartij verstrekte informatie, tenzij wederpartij weet of redelijkerwijs behoort te weten dat de verkregen informatie onjuist is."
5	Juridisch	Eerste NvI vraag 17:	In uw antwoord geeft u aan dat u er niet mee bekend bent dat de uitvoering van deze opdracht uitgevoerd wordt met inachtneming van gedrags- en beroepsregels. De door u uitgevraagde werkzaamheden worden, indien wij de opdracht gegund zouden krijgen, (mede) uitgevoerd door medewerkers met een RE-titel (Register EDP-Auditor). Een RE is ingeschreven in het register van de Beroepsorganisatie van IT-Auditors (NOREA). Dit brengt met zich mee dat deze medewerkers bij de uitvoering van de opdracht gebonden zijn aan de NOREA gedrags- en beroepsregels. De door ons voorgestelde toevoeging is derhalve relevant en noodzakelijk. Wij willen u daarom vragen om alsnog te bevestigen dat in de zin van dit artikel onder wettelijke voorschriften eveneens wordt begrepen de toepasselijke gedrags- en beroepsregels?	Dat bevestigen wij niet. De voor de opdracht niet per se noodzakelijke beroeps- en gedragsregels stellen wij immers niet op een lijn met (de) wettelijke voorschriften. Bij de thans aanbestede opdracht zal wederpartij (opdrachtnemer) echter door ons nooit verplicht worden om in strijd te handelen met (zijn) toepasselijke gedrags- en beroepsregels.
6	Juridisch	Eerste NvI vraag 14:	Wij begrijpen dat u gezien het karakter van de opdracht een boete op de geheimhoudingsplicht wilt hanteren. Echter, een boete heeft een puur punitief karakter aangezien er geen samenhang is met eventueel geleden schade. Ook zonder dat er sprake is van geleden schade kan er sprake zijn van het verbeuren van een boete. De huidige boete achten wij zeer hoog en daarmee buiten proportioneel. Wij menen dat het hanteren van een (enigszins) lagere boete geen afbreuk doet aan het afschrikwekkende karakter daarvan. Wij willen u derhalve vragen om de boete te halveren tot een bedrag van € 25.000 per gebeurtenis. Ons inziens wordt hiermee voldoende recht gedaan aan de aard van de opdracht en de afschrikwekkende werking van een boete maar is er tevens sprake van een proportionele boete. Kunt u hiermee instemmen?	Ja, daar stemmen wij mee in. Het in artikel 17.5 ARBIT-2022 genoemde boetebedrag van € 50.000,- per overtreding is thans gewijzigd in € 25.000,- per overtreding.
7	Juridisch	Eerste NvI, vraag 9	Artikel 26.4 sub d noemt inderdaad geen vrijwaring maar een situatie waarin de aansprakelijkheidsbeperking niet van toepassing is. De eerste zin van dit artikel is conform het bepaalde in artikel 82 lid 2 AVG. De tweede zin van artikel 26.4 sub d, inzake boetes, is echter niet conform de werking van de AVG. Boetes die opgelegd kunnen worden door een toezichthoudende autoriteit zijn geregeld in artikel 83 AVG. Boetes kunnen opgelegd worden aan een verwerker of een verwerkingsverantwoordelijke indien er gehandeld is in strijd met een (beboetbare) verplichting op grond van de AVG. De door u opgenomen zin suggereert echter dat een partij een boete opgelegd kan krijgen die toerekenbaar is aan een andere partij en dat de eerste partij daarom het recht moet hebben om de boete te verhalen. Er is echter geen juridische grondslag op grond waarvan de opdrachtgever een boete opgelegd krijgt die toerekenbaar is aan opdrachtnemer. Opdrachtgever kan alleen een boete opgelegd krijgen indien zij zelf een op haar rustende verplichting geschonden heeft. Dit geldt ongeacht of er sprake is van een verwerker – verwerkingsverantwoordelijke verhouding tussen partijen of dat er sprake is van een verhouding tussen twee verwerkingsverantwoordelijken. Wij vragen u derhalve de volgende zin buiten toepassing te verklaren aangezien dit niet conform de wettelijke werking is: "Onder schade wordt mede begrepen een door de toezichthoudende autoriteit opgelegde boete." Kunt u hiermee instemmen? Zo niet, kunt u aangeven onder welke omstandigheden u	Nee, daar stemmen wij niet mee in. De vraag geeft geen aanleiding ons eerdere antwoord op vraag 9 van Nota van inlichtingen-1 te (moeten) wijzigen. Verder is het niet ondenkbaar, dat wij schade kunnen ondervinden van, of een boete opgelegd kunnen krijgen, als gevolg van een schending van wet- en regelgeving op het terrein van de bescherming van persoonsgegevens door de wederpartij (opdrachtnemer). Overigens is een verwerkersovereenkomst, en dus van 'rechtmatige instructies van de verwerkingsverantwoordelijke', nog niet aan de orde bij onderhavige opdracht. Zie bijvoorbeeld vraag en antwoord 25 van Nota van inlichtingen-1 .

8	Juridisch	Eerste NvI, vraag 7:	In uw antwoord geeft u aan dat er verzekeringen in de branche bestaan met de gevraagde dekking en dat deze voorwaarden daarom van een professionele partij verlangd kunnen worden. Ten aanzien van de hoogte van de dekking zijn wij dat mij u eens en voldoen wij ook ruimschoots aan het gevraagde. In artikel 29.3 wordt echter ook gevraagd om, op uw verzoek, mededeling doet van eerdere claims onder dezelfde polis in het lopende verzekeringsjaar. Het doen van een dergelijke mededeling is niet gebruikelijk binnen de markt/branche en achten wij ook bedrijfsvertrouwelijke informatie. Het is ons inziens voor u ook niet relevant of er eerder claims onder dezelfde polis gedaan zijn zolang dit maar geen afbreuk doet aan de verplichting om adequaat verzekerd te zijn jegens u en de bij u uitgevoerde opdracht. Wij wensen derhalve de volgende tekst in artikel 29.3 buiten toepassing verklaren: “mededeling doet van eerdere claims onder dezelfde polis in het lopende verzekeringsjaar”. Kunt u hiermee instemmen?	Ja, daar stemmen wij mee in. Artikel 29.3 ARBIT-2022 is thans als volgt gewijzigd: "Wederpartij overlegt op verzoek onverwijld bewijs van premiebetaling aan opdrachtgever."
9	Juridisch	Eerste NvI, vraag 6:	In uw antwoord geeft u aan dat u er niet mee bekend bent dat de uitvoering van deze opdracht uitgevoerd wordt met inachtneming van gedrags- en beroepsregels en door beroepsbeoefenaren. De door u uitgevraagde werkzaamheden worden, indien wij de opdracht gegund zouden krijgen, (mede) uitgevoerd door medewerkers met een RE-titel (Register EDP-Auditor). Een RE is ingeschreven in het register van de Beroepsorganisatie van IT-Auditors (NOREA) en zijn dus beroepsbeoefenaren. Dit brengt met zich mee dat deze medewerkers bij de uitvoering van de opdracht gebonden zijn aan de NOREA gedrags- en beroepsregels. De door ons voorgestelde toevoeging is derhalve relevant en noodzakelijk. Wij willen u daarom vragen om alsnog akkoord te gaan met ons eerdere tekstvoorstel?	Wij gaan niet akkoord met het eerder gedane tekstvoorstel. De voor de opdracht niet per se noodzakelijke beroeps- en gedragsregels stellen wij immers niet op een lijn met (de) wettelijke voorschriften. Bij de thans aanbestede opdracht zal wederpartij (opdrachtnemer) echter door ons nooit verplicht worden om in strijd te handelen met (zijn) toepasselijke gedrags- en beroepsregels.
10	Juridisch	Nvi #1, vraag 25 Verwerkersovereenkomst	Bijlage I – Verwerkersovereenkomst - Artikel 12.1, 15.2 In artikel 12 wordt Opdrachtnemer gevraagd potentiële datalekken binnen 24 uur te melden. Gezien de grootte van de organisatie van Opdrachtnemer en de stakeholders die betrokken dienen te worden is deze termijn niet acceptabel. Is het akkoord om deze termijn aan te passen naar 48 uur? Ook wordt in artikel 12 gesproken van mogelijke incidenten en security incidenten. Opdrachtnemer is verplicht om daadwerkelijke datalekken die impact op de bescherming van persoonsgegevens hebben te melden. In gevallen waar Opdrachtnemer incidenten of aanvallen op de beveiliging succesvol afweerd of behandeld, incidenten die die als beveiligingsincident aangemerkt kunnen worden maar niet zijn aan te merken als datalek zal Opdrachtnemer de incidenten niet melden nu deze geen impact hebben op de veiligheid van de gegevens en dit leidt tot een onredelijke meldplicht. Opdrachtnemer zal daadwerkelijke datalekken uiteraard altijd tijdig bij Opdrachtgever melden. Is het in dit kader akkoord op “(Mogelijke) gebeurtenis die plaatsvindt door techniek of door menselijk handelen waarbij de Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van data/informatie en/of de systemen/applicaties van VfPf wordt verstoord (security incident) evenals bij een dergelijke gebeurtenis persoonsgegevens betrokken zijn (datalek).” te verwijderen en te vervangen met “datalek”? En “mogelijke” uit de laatste zin te verwijderen? Is het in dit kader ook akkoord om (mogelijk) uit artikel 15.2 te verwijderen?	Opdrachtgever is als verwerkingsverantwoordelijk gehouden om meldingsplichtige datalekken binnen 72 uur te melden. De opgenomen tijd van 24 uur is hierbij een redelijke tijd, gelet op de aard van de melding. Opdrachtgever is de partij die vaststelt of sprake is van security incidenten, meer concreet Team P&S is verantwoordelijk voor de inhoudelijke conclusie(s). Om dat te kunnen doen is het nodig dat alle security gebeurtenissen (een omstandigheid waarbij mogelijk sprake is van een inbreuk op de beschikbaarheid, integriteit en/of vertrouwelijkheid van data/informatie van VfPf op systemen/applicaties van of namens VfPf) gemeld worden. Een melding van opdrachtnemer is in de ogen van opdrachtgever dus een eerste melding c.q. een signaal (twijfels, voorspellingen, mogelijkheden etc.) van een security gebeurtenis. Het gaat erom dat opdrachtgever onverwijld op de hoogte gesteld wordt van gebeurtenissen om vervolgens met elkaar de verdere route te bepalen. Qua melding is opdrachtnemer gehouden om niet alleen datalekken te melden. Alle security gebeurtenissen die zich binnen de opdracht afspelen moeten worden gemeld. Opdrachtgever is verantwoordelijk voor alle gebeurtenissen, op grond van de AVG en op grond van de behaalde ISO27001 certificering incl. bijbehorende beheersmaatregelen. Dit is opgenomen in het beleid opdrachtgever (Incident response plan). De voorstellen worden afgewezen.
11	Juridisch	Nvi #1, vraag 25 Verwerkersovereenkomst	Bijlage I – Verwerkersovereenkomst – Artikel 16 Het is voor Opdrachtnemer niet akkoord om onbeperkte aansprakelijkheid voor data privacy breaches te accepteren. Het aansprakelijkheidsrisico dient redelijkerwijs gekoppeld te zijn aan de fees van de betreffende opdracht. Is het in dat kader akkoord om het volgende artikel toe te voegen aan artikel 16? 16.5. De aansprakelijkheid van Opdrachtnemer onder deze Verwerkersovereenkomst is beperkt tot drie maal de waarde van de opdracht.	Nee, daar stemmen wij niet mee in. De vraag geeft geen aanleiding ons eerdere antwoord te (moeten) wijzigen. Het is immers niet ondenkbaar dat wij schade kunnen ondervinden van of een boete opgelegd kunnen krijgen, als gevolg van een schending van wet- en regelgeving op het terrein van de bescherming van persoonsgegevens door de wederpartij (opdrachtnemer). Overigens is een verwerkersovereenkomst nog niet aan de orde bij onderhavige opdracht. Overigens zij verwezen naar alle andere antwoorden over het onderwerp aansprakelijkheid.

12	Juridisch	Nvi #1, vraag 25 Verwerkersovereenkomst	In artikel 14 wordt Opdrachtnemer gevraagd persoonsgegevens op verzoek permanent te verwijderen. In bepaalde gevallen is het technisch niet mogelijk om persoonsgegevens direct permanent te verwijderen van onze systemen, omdat er met oog op de beveiliging en beschikbaarheid van de gegevens sprake is van een back-up termijn van twee maanden, waarbij de back-up niet direct verwijderd kan worden. Wel kunnen wij bevestigen dat het proces van verwijdering in gang is gezet. Daarnaast geldt dat het verwijderen van de persoonsgegevens in bepaalde gevallen in strijd kan zijn met retentieverplichtingen onder toepasselijke wetgeving. Is het in dat kader akkoord om het volgende toe te voegen aan artikel 14? Bij beëindiging, ontbinding of opzegging van deze Overeenkomst, op verzoek, op welke grond of wijze dan ook, zal Verwerker op eerste verzoek van Verwerkingsverantwoordelijke, tenzij toepasselijke wetgeving zich hiertegen verzet, (i) aan Verwerkingsverantwoordelijke alle persoonsgegevens en overige aan Verwerkingsverantwoordelijke toekomende gegevens ter beschikking stellen op de wijze en in het format dat Verwerkingsverantwoordelijke wenst, (ii) per direct de verwerking van de persoonsgegevens staken, (iii) alle documenten waarin de persoonsgegevens zijn vastgelegd aan Verwerkingsverantwoordelijke ter beschikking stellen, en (iv) alle persoonsgegevens die elektronisch zijn opgeslagen permanent van de gegevensdrager verwijderen, of voor zover permanente verwijdering van de gegevensdrager niet mogelijk is, de gegevensdrager vernietigen. Dit geldt niet voor back-ups van elektronisch opgeslagen persoonsgegevens welke vanuit technisch oogpunt niet direct verwijderd kunnen worden, waarvoor een maximale verwijdertermijn van twee maanden geldt.	Het verwijderen van (persoons) gegevens zal altijd in lijn met de retentie-eisen en bewaartermijn van opdrachtgever moeten geschieden. Het betreft dan eisen binnen de scope van de opdracht. Dat laat onverlet dat opdrachtnemer ook eigen eisen en verantwoordelijkheden op dit gebied heeft. Op dit moment valt nog niet vast te stellen wat de impact van het voorstel is op opdrachtgever. Om die reden wordt het voorstel afgewezen. Opdrachtgever zegt toe te allen tijde het gesprek aan te gaan over het verwijderen van (persoons)gegevens en de wijze waarop dit gestalte gegeven wordt. Het is daarbij aan de procesketeneigenaren van opdrachtgever om het risico ervan te bepalen en door hen te laten beslissen of er afwijkingen (zoals voorgesteld door opdrachtnemer) geaccepteerd worden.
13	Juridisch	Nvl #1, vraag 25 Verwerkersovereenkomst	Bijlage I – Verwerkersovereenkomst - Artikel 3.2, 6.1, 6.2 In de verwerkersovereenkomst wordt Opdrachtnemer beperkt om persoonsgegevens voor andere doeleinden te verwerken dan door de verantwoordelijke vastgesteld. Voor een goede dienstverlening en bedrijfsvoering van Opdrachtnemer is deze omschrijving te beperkt. Is akkoord om aan deze bepaling toe te voegen dat Opdrachtnemer persoonsgegevens mag vewerken voor de volgende doeleinden?: Het uitvoeren van de opdracht, risk management en quality review vereisten, interne zakelijke doeleinden, het voeldoen aan toepasselijke wet- en (beroeps) regelgeving, en in verband met een tucht-, civiel-, bestuurs- en/of strafrechtelijke procedure (een juridische procedure) waar Opdrachtnemer of personen verbonden aan of werkzaam bij Opdrachtnemer betrokken zijn en waarbij deze informatie van belang kan zijn.	De invulling van de verwerkersovereenkomst is op dit moment nog niet aan de orde. Immers, het is in de basis de bedoeling dat opdrachtnemer zich richt op de doelstellingen uit deze opdracht. Het verwerken van persoonsgegevens is nog niet aan de orde. Of sprake is van een mogelijke verwerking is op voorhand niet te voorspellen, evenmin wat die verwerking dan precies behelst. Om die reden is het voor nu te opportuun om de scope al voortijdig vast te leggen. Opdrachtgever zegt toe om du moment de verwerking aanstonds is, de omschrijving te bepalen op de thans aanwezige omstandigheden, waarbij overigens de voorgestelde passage een goed vertrekpunt kan zijn. Het voorstel wordt afgewezen.
14	Juridisch	Nvi #1, vraag 25 Verwerkersovereenkomst	Bijlage I – Verwerkersovereenkomst - Artikel 7.1 - 7.3 In deze bepaling wordt Opdrachtnemer beperkt in het internationaal uitwisselen van persoonsgegevens. Opdrachtnemer is een onderdeel van een internationaal netwerk van firms. Voor een goede uitvoering van de dienstverlening is het noodzakelijk dat Opdrachtnemer zonder toestemming persoonsgegevens kan uitwisselen. Daarbij maakt Opdrachtnemer gebruik van ICT-dienstverleners die de technische omgeving van Opdrachtnemer faciliteren, welke noodzakelijk zijn om de opdracht uit te kunnen voeren. Is het in dat kader akkoord om Artikel 7.1-7.3 te vervangen met het volgende? Opdrachtnemer zal persoonsgegevens alleen naar landen buiten de EER sturen indien de ontvanger geacht wordt een passend beschermingsniveau van gegevensbescherming te bieden op grond van de AVG. Op basis van de intra-network data transfer agreement (“INTA”) is het Opdrachtnemer toegestaan persoonsgegevens te versturen binnen het netwerk van <OPDRACHTNEMER> firms.	Opdrachtgever houdt vast aan de eisen uit de verwerkersovereenkomst. In de verwerkersovereenkomst wordt aangegeven dat opdrachtgever altijd toestemming kan geven als daarom gevraagd wordt. Het is voor opdrachtgever onmogelijk om op basis van de toelichting van opdrachtnemer op voorhand al toezeggingen te doen. Opdrachtgever wijst het voorstel van de hand maar zegt toe altijd in gesprek te gaan met opdrachtnemer over dergelijke verzoeken. Als opdrachtgever daartoe over gaat dan zal dit altijd geschieden conform de eisen uit de verwerkersovereenkomst, meer in het bijzonder op basis van instructies van opdrachtgever.

15	Juridisch	Nvi #1, vraag 25 Verwerkersovereenkomst	In de verwerkersovereenkomst (Bijlage I – Verwerkersovereenkomst - Artikel 3.2, 6.1, 6.2) wordt Opdrachtnemer beperkt om persoonsgegevens voor andere doeleinden te verwerken dan door de verantwoordelijke vastgesteld. Voor een goede dienstverlening en bedrijfsvoering van Opdrachtnemer is deze omschrijving te beperkt. Is akkoord om aan deze bepaling toe te voegen dat Opdrachtnemer persoonsgegevens mag vewerken voor de volgende doeleinden?: Het uitvoeren van de opdracht, risk management en quality review vereisten, interne zakelijke doeleinden, het voldoen aan toepasselijke wet- en (beroeps) regelgeving, en in verband met een tucht-, civiel-, bestuurs- en/of strafrechtelijke procedure (een juridische procedure) waar Opdrachtnemer of personen verbonden aan of werkzaam bij Opdrachtnemer betrokken zijn en waarbij deze informatie van belang kan zijn.	De invulling van de verwerkersovereenkomst is op dit moment nog niet aan de orde. Immers, het is in de basis de bedoeling dat opdrachtnemer zich richt op de doelstellingen uit deze opdracht. Het verwerken van persoonsgegevens is nog niet aan de orde. Of sprake is van een mogelijke verwerking is op voorhand niet te voorspellen, evenmin wat die verwerking dan precies behelst. Om die reden is het voor nu te opportuun om de scope al voortijdig vast te leggen. Opdrachtgever zegt toe om du moment de verwerking aanstonds is, de omschrijving te bepalen op de thans aanwezige omstandigheden, waarbij overigens de voorgestelde passage een goed middel ter inspiratie kan dienen. Het voorstel wordt afgewezen.
16	Juridisch	Nvl #1, vraag 21 Vrijwaring	Ontbrekende bepalingen. Wij stellen voor om onderstaande bepalingen aanvullend in de te sluiten (nadere) overeenkomst op te nemen ten aanzien van de dienstverlening die ziet op beoordelingen. Deze specifieke bepalingen zijn gebruikelijk en van zeer groot belang bij o.a. IT-penetratietesten. Kunt u hiermee akkoord gaan? “Opdrachtgever stemt uitdrukkelijk in met het uitvoeren van de met opdrachtnemer overeengekomen werkzaamheden op de door Opdrachtgever aangewezen delen van zijn ICT-systemen. Opdrachtgever staat ervoor in dat een eventuele internet service provider waar de onderzoeksobjecten zijn gehost op de hoogte is gesteld van het uitvoeren van deze penetratietest en met de uitvoering daarvan uitdrukkelijk heeft ingestemd.” “Opdrachtgever is ervan op de hoogte dat het uitvoeren van de beveiligingstesten kan leiden tot wijziging of verlies van gegevens. Tenzij sprake is van opzet of bewuste roekeloosheid zijdens opdrachtnemer, is opdrachtnemer niet aansprakelijk voor enige (directe en indirecte) schade, gevolgschade en schade voortvloeiende uit aanspraken van derden daaronder begrepen, veroorzaakt door het analyseren en/of het binnendringen dan wel iedere poging tot het analyseren en/of binnendringen van de ICT-systemen van opdrachtgever, onder de uitdrukkelijke voorwaarde dat opdrachtnemer uitsluitend de beveiliging tracht te analyseren en/of tracht te doorbreken en/of toegang tracht te verwerven tot door (opdrachtgever) aangegeven onderdelen van het geautomatiseerd werk. Deze uitsluiting van de aansprakelijkheid geldt uitsluitend voor zover opdrachtnemer handelt in overeenstemming met de schriftelijke opdracht van de opdrachtgever. De opdrachtgever zal zorgdragen voor een volledige back-up van alle gegevens die op haar netwerken en/of systemen zijn opgeslagen.” “Opdrachtgever vrijwaart opdrachtnemer terzake van vorderingen van derden (waaronder eventuele kosten van rechtsbijstand, indien nodig) in verband met (pogingen tot) het analyseren en/of binnendringen van het geautomatiseerde werk van de opdrachtgever, voor zover de opdrachtnemer deze handelingen verricht in opdracht van de opdrachtgever.” Daarnaast hebben wij grond van de op onze organisatie toepasselijke wet- en (beroeps)regelgeving hebben wij uw uitdrukkelijke toestemming nodig om de betreffende informatie te mogen delen met IT (cloud) dienstverleners	Nee, daar kunnen wij niet mee akkoord gaan. Dat is thans te voorbarig, en sommige met de vraag voorgestelde bepalingen zijn ook niet noodzakelijk. Wij begrijpen (echter) wel, dat de (eventuele) uitvoering van IT-penetratietesten (zie vraag en antwoord 72 Nota van inlichtingen-1) om duidelijke afspraken tussen, en spelregels voor, opdrachtgever en wederpartij (opdrachtnemer) vraagt. In geval van de uitvoering van een IT-penetratietest zullen wij dan (steeds) ook voorafgaand in goed onderling overleg met de wederpartij gaan om de betreffende afspraken en spelregels adequaat en naar tevredenheid van beide partijen vast te leggen.

			informatie te mogen delen met IT (cloud) dienstverleners. Voor (de uitvoering van) haar dienstverlening maakt Opdrachtnemer gebruik van cloud-toepassingen, e-mailproviders en andere ondersteunende IT (cloud) dienstverleners, onder meer voor onze document managementsystemen, waarbij dossiers en (klant)informatie worden opgeslagen in de cloud. Voor de zeer beperkte gevallen dat deze IT (cloud) dienstverleners, in verband met noodzakelijke technische ondersteuning, beperkte inzage hebben in de vertrouwelijke (klant)informatie, gelden strikte geheimhoudingsafspraken. Voor de goede orde benadrukken wij dat de ondersteuning van onze interne bedrijfsprocessen door betreffende IT (cloud) dienstverleners noodzakelijk is voor de uitvoering van onze dienstverlening, waarbij wij verantwoordelijkheid aanvaarden voor de inzet van deze IT (cloud) dienstverleners en de (de handhaving van de) vertrouwelijkheid van de (klant)informatie. Op grond van het voorgaande verzoeken wij u onderstaand tekstvoorstel op te nemen in de te sluiten overeenkomst. Zonder uw uitdrukkelijke toestemming kan Opdrachtnemer de werkzaamheden niet uitvoeren. Kunt u akkoord gaan met het opnemen van onderstaande bepaling in de Overeenkomst? “Ten behoeve van (de uitvoering van) de Opdracht kunnen Opdrachtgever en Opdrachtnemer door middel van elektronische middelen met elkaar communiceren en/of gebruik maken van elektronische opslag (waaronder cloud-toepassingen), waarbij het Opdrachtnemer is toegestaan vertrouwelijke informatie te verstrekken aan IT (cloud) dienstverleners, op basis van vertrouwelijkheid en uitsluitend ter ondersteuning van de bedrijfsvoering van Opdrachtnemer. Opdrachtnemer blijft jegens	
17	Juridisch	Nvi #1, vraag 10 Aansprakelijkheid	Beperking van aansprakelijkheid (Artikel 26.2 en 26.3 ARBIT-2022). In uw antwoord op vraag 10 geeft u aan niet in te stemmen met het aanpassen van de beperking van aansprakelijkheid zoals opgenomen in artikel 26.2 en 26.3 ARBIT-2022, waarbij u o.a. aangeeft dat dit niet noodzakelijk is, omdat de schade verzekerbaar zou zijn. Graag wijzen wij u echter op Voorschrift 3.9 D van de Gids Proportionaliteit die in januari 2022 door het Ministerie van Economische Zaken en Klimaat is uitgebracht. Dit Voorschrift 3.9 D bepaalt dat de aansprakelijkheid van de opdrachtnemer gelimiteerd dient te zijn, waarbij de aansprakelijkheidsbeperking die in de betreffende branche gebruikelijk is in acht dient te worden genomen. Zoals aangegeven is een beperking van aansprakelijkheid van 3x de fee gangbaar bij adviesdiensten (en voor het leveren van IT geldt een branchegebruik van 1x de fee). Derhalve willen wij u vragen of u akkoord kunt gaan met het opnemen van onderstaande, marktconforme, bepaling in de Overeenkomst ter vervanging van artikel 26.2 en 26.3 ARBIT-2022: “Opdrachtnemer zal zijn werkzaamheden naar beste kunnen verrichten en daarbij de zorgvuldigheid in acht nemen die van Opdrachtnemer kan worden verwacht. Indien een fout wordt gemaakt doordat Opdrachtgever aan Opdrachtnemer onjuiste of onvolledige informatie heeft verstrekt, is Opdrachtnemer voor de daardoor ontstane schade niet aansprakelijk. Indien de Opdrachtgever aantoont dat hij schade heeft geleden door een fout van Opdrachtnemer die bij zorgvuldig handelen zou zijn vermeden, is Opdrachtnemer voor die schade aansprakelijk tot maximaal het bedrag van het honorarium dat opdrachtgever aan opdrachtnemer heeft betaald en/of nog verschuldigd is over de laatste twaalf maanden voor de onder de opdracht verrichte specifieke werkzaamheden waaruit de fout voortvloeit. Samenhangende fouten worden daarbij aangemerkt als één fout. De beperking van aansprakelijkheid geldt niet indien er sprake is van opzet of bewuste roekeloosheid aan de zijde van opdrachtnemer en/of indien dwingende (inter)nationale wet- of (beroeps) regelgeving een dergelijke beperking niet toestaat. Opdrachtnemer is niet aansprakelijk voor gevolg-, indirecte, bedrijfs- of strafschade en/of winstderving.”	Nee, daartoe bestaat immers geen nut, noch een noodzaak. De vraag geeft geen aanleiding ons eerdere antwoord op vraag 10 van Nota van inlichtingen-1 te (moeten) wijzigen. De artikelen 26.2 en 26.3 ARBIT-2022 zijn niet in strijd met het bepaalde in de Gids Proportionaliteit en geven bijvoorbeeld (al) een 'limitering' (beperking) zoals (onder meer) gebruikelijk in de IT Branche. Een deel van de vraag wordt overigens al ondervangen door de toepassing van het Burgerlijk Wetboek op de opdracht.

18	Juridisch	Nvi #1, vraag 16 Auditrecht	Toezicht (Artikel 17.3 ARBIT). Generlei beperking / inperking van het auditrecht van Opdrachtgever is voor ons niet acceptabel op grond van van toepassing zijnde wet- en beroepsregels (binnen ons concern worden ook accountantsdiensten en belastingadviesdiensten geleverd) en de daaruit voortvloeiende geheimhoudingsverplichtingen die wij als organisatie ten aanzien van onze administratie en onze dossiers in acht dienen te nemen en is voorts in strijd met onze contractuele geheimhoudingsverplichtingen jegens andere Opdrachtgevers en relaties. Kunt u bevestigen dat waar geheimhouding nodig is, Opdrachtgever akkoord gaat met een beperking / inperking van het auditrecht ten aanzien van alleen die informatie ten aanzien waarvan wij op grond van bovenstaande geheimhouding behoeven? Wij zouden dit als volgt wensen vorm te geven: De Opdrachtnemer zal te allen tijde meewerken aan audits die worden uitgevoerd door onafhankelijke accountants van Opdrachtgever, voldoende middelen ter beschikking stellen om de audit te faciliteren, waaronder in ieder geval: a) toegang tot het personeel van Opdrachtnemer dat betrokken is bij de levering van Diensten aan Opdrachtgever om de naleving van de Overeenkomst door Opdrachtnemer te beoordelen; b) redelijkerwijs vereiste documentatie om de naleving van de Overeenkomst door Opdrachtnemer aan te tonen (met uitzondering van de werkdocumenten van de Opdrachtnemer en het interne beleid van Opdrachtnemer); en c) een financiële boekhouding met betrekking tot de facturering, zoals urenstaten en onkostenstaten, maar geen informatie over salarissen, algemene kosten of voordelen; en d) toegang tot geschikt personeel dat betrokken is bij het beheer van IT-systemen om de IT-omgeving van de Opdrachtnemer en de veiligheidscontroles te bespreken. Overeengekomen wordt dat Opdrachtgever (en diens accountant) alleen toegang hebben tot de algemene (vergader)ruimten van de Opdrachtnemer binnen het pand van de Opdrachtnemer waar geen vertrouwelijke (klant)informatie aanwezig zal zijn. Overeengekomen is dat de werkdocumenten van de Opdrachtnemer de vertrouwelijke en bedrijfseigen informatie van de Opdrachtnemer zijn en niet aan Opdrachtgever worden verstrekt en dat de Opdrachtnemer niet verplicht is om informatie bekend te maken die de Opdrachtnemer in strijd met haar eigen geheimhoudingsverplichtingen zou plaatsen. De Opdrachtnemer is niet verplicht de bepalingen van artikel 17 ARBIT-2022 en deze aanvullende bepaling na te leven wanneer het onderwerp van een verzoek om informatie/uitvoering van een kwaliteitscontrole betrekking heeft op een zaak die het onderwerp is van een geschil dat betrekking heeft op een lopende of hangende rechtszaak tussen Opdrachtgever en de Opdrachtnemer, of die, op basis van de waarschijnlijkheid, zal leiden tot een rechtszaak tussen Opdrachtgever en de Opdrachtnemer en die de positie van de Opdrachtnemer in gevaar zou kunnen brengen. Kunt u hiermee akkoord gaan?	Het auditrecht is een recht dat opdrachtgever nodig heeft om zichzelf te kunnen verzekeren dat afspraken nagekomen worden. Een beperking hierop acht opdrachtgever niet redelijk en ook hoogst ongebruikelijk gelet op de wijze waarop opdrachtgever aankijkt tegen informatiebeveiliging zoals is neergelegd in onze ISO27001-werkwijze en inzichten. Opdrachtgever realiseert zich dat documenten vanwege aparte op opdrachtnemer rustende wettelijke verplichtingen en verantwoordelijkheden om die andere redenen ontoegankelijk zijn. Opdrachtgever acht nu niet het moment om beperkingen aan te brengen in dit auditrecht, wetende dat nog niet duidelijk is waarop een audit zal plaatsvinden. Opdrachtgever zegt toe dat een audit die door opdrachtgever ingezet wordt richting opdrachtnemer altijd rekening houdt met de op opdrachtnemer rustende wettelijke verplichtingen en geheimhoudingen, zolang de doelen van de audit en het voor opdrachtgever te bereiken resultaat hiermee niet interfereert.
19	Juridisch	Nvi #1, vraag 7, Melding claims onder verzekeringspolis	Melding claims onder verzekeringspolis (Artikel 29.2 en 29.3 ARBIT). In uw beantwoording van vraag 7 gaat u niet in op het aanbod om een verklaring van de verzekeraar te overleggen waaruit adequate verzekering blijkt. Op grond van contractuele afspraken met onze verzekeraar mogen wij derden (waaronder cliënten) geen informatie verstrekken omtrent eerdere claims onder dezelfde polis. Indien wij een certificaat verstrekken van onze verzekeringsagent waaruit blijkt dat wij genoegzaam verzekerd zijn en de verzekeringspremie hebben betaald, kunt u dan akkoord gaan met het in overeenkomst de te sluiten Overeenkomst buiten toepassing verklaren in van de verplichting om ‘mededeling te doen van eerdere claims onder dezelfde polis in het lopende verzekeringsjaar’ conform artikel 29.3 ARBIT-2022?	Ja, daar gaan wij mee akkoord. Artikel 29.3 ARBIT-2022 is thans als volgt gewijzigd: "Wederpartij overlegt op verzoek onverwijld bewijs van premiebetaling aan opdrachtgever."
20	Juridisch	Nvi #1, vraag 9 Aansprakelijkheid	Onbeperkte aansprakelijkheid voor o.a. privacy (Artikel 26.4.d ARBIT). In uw antwoord op vraag 9 geeft u aan artikel 26.4 sub d ARVODI-2022 te handhaven en geeft u terecht aan dat u ARBIT-2022 hanteert en niet ARBIT-2018. In dat kader het volgende. Een dergelijke onbeperkte aansprakelijkheid is zeer ongebruikelijk in onze branche. Het risico dat op deze manier bij de opdrachtnemer wordt neergelegd is bovendien disproportioneel, aangezien dit vrijwel onverzekerbaar is en daarnaast niet verdisconteerd in onze fees. Kunt u akkoord gaan met het buiten toepassing verklaren van dit artikel 26.4 sub d?	Nee, daartoe bestaat geen nut, noch een noodzaak. De aanname dat sprake is van (een) ‘onbeperkte aansprakelijkheid’ is immers onjuist. Van ‘disproportionaliteit’ is daarbij (dus) ook geen sprake, omdat het Burgerlijk Wetboek (ook) van toepassing is op de (aanbestede) Overeenkomst. Dus ook op het bepaalde in artikel 26.4 ARBIT-2022. Zie daartoe bijvoorbeeld ook prof. mr. C.E.C. Jansen in het Tijdschrift voor Bouwrecht (TBR 2016, 4, pag. 335 en 337). En zie ook Rechtbank Zeeland-West-Brabant 6 november 2014, ECLI:NL:RBZWB:2014:7530. Verder is het niet ondenkbaar, dat wij schade kunnen ondervinden van, of een boete opgelegd kunnen krijgen, als gevolg van een schending van wet- en regelgeving op het terrein van de bescherming van persoonsgegevens door de wederpartij (opdrachtnemer). Overigens is een verwerkersovereenkomst, en dus van 'rechtmatige instructies van de verwerkingsverantwoordelijke', nog niet aan de orde bij onderhavige opdracht. Zie bijvoorbeeld vraag en antwoord 25 van Nota van inlichtingen-1 .

21	Juridisch	Nvi #1, vraag 2 Rechtsgeldige ondertekening	Rechtsgeldige ondertekening (Offerteaanvraag § 2.9 stap 1). In uw antwoord op vraag 2 geeft u aan dat het gebruik van een digitale handtekening is toegestaan, mits ondertekening plaatsvindt door een blijkens het handelsregister bevoegd persoon. Wij willen de offerte, inclusief het Uniform Europees Aanbestedingsdocument, laten ondertekenen door de eindverantwoordelijke partner of director. Partners/directors staan echter niet op het uittreksel van de Kamer van Koophandel vermeld als rechtsgeldig vertegenwoordiger. Volstaat voor rechtsgeldige ondertekening een volmachtverklaring van de bestuurders (wel genoemd in het uittreksel van de Kamer van Koophandel) dat desbetreffende partner/director bevoegd is te tekenen en zo ja, wilt u dat wij deze volmachtverklaring bij de offerte voegen? Kunt u in dat kader toestaan dat de offerte en de bijlagen, waaronder ook het Uniform Europees Aanbestedingsdocument, ondertekend worden door de eindverantwoordelijke partner/director?	Ja, dat is akkoord en staan wij toe. De betreffende volmacht moet bij de inschrijving worden gevoegd.