

## Programma van Eisen

### Algemeen

1. Opdrachtnemer garandeert dat het door Opdrachtnemer te leveren repowerwerk gedurende de looptijd van de Raamovereenkomst van onveranderde goede kwaliteit is en blijft. Het product voldoet in alle opzichten aan de gebruikelijke eisen van de wet- en regelgeving (in het kader van veiligheid), Arbo, deugdelijkheid, doelmatigheid, taakgeschiktheid, afwerking, normen, specificaties, overheidsvoorschriften en milieubepalingen.
2. Opdrachtnemer houdt zich aan de minimeisen van de landelijke criteria voor maatschappelijk verantwoord inkopen (MVI) ten aanzien van duurzaamheid. Deze zijn als bijlage toegevoegd aan de aanbestedingsdocumenten.
3. Opdrachtnemer voorziet Opdrachtgever van een online bestelportaal.
4. Opdrachtnemer staat garant voor een constante kleurbalans over de gehele oplaat volgens de normvellen.
5. Uitleveren van de Opdrachten geschiedt op volledige verantwoording van de Opdrachtnemer.
6. Van opdrachtverstrekking tot levering wijst Opdrachtnemer een vaste contactpersoon en een vaste vervanger aan die de contacten met Opdrachtgever onderhoudt en aanspreekbaar is voor alle voorkomende zaken.
7. Een accountmanager c.q. vast contactpersoon van Opdrachtnemer dient de dienstverlening en de geleverde kwaliteit halfjaarlijks te evalueren. Hiervoor worden vanuit Opdrachtnemer kosteloos management rapportages opgesteld. Over de inhoud van de management rapportages worden nadere afspraken gemaakt na ondertekening van het contract. Tijdens de halfjaarlijkse evaluatie worden verder nog de kwaliteit van de dienstverlening en recente marktontwikkelingen besproken.
8. Indien Opdrachtgever niet tevreden is over de accountmanager c.q. vast contactpersoon van Opdrachtnemer, behoudt Opdrachtgever zich het recht voor een andere accountmanager en/of contactpersoon te kiezen.
9. Inhoudelijk dient de Opdrachtnemer er mee in te stemmen dat binnen een af te sluiten SLA, KPI's worden geconcretiseerd en praktijkafspraken worden vastgelegd.
10. Opdrachtnemer voldoet aan de vastgestelde kwaliteitseisen, deze zijn vastgelegd doordat de Opdrachtnemer zich heeft geconformeerd middels de productie van de normvellen.
11. Van Opdrachtnemer wordt een adviserende houding verwacht met betrekking tot de bestellingen.

### Drukproef

12. Opdrachtnemer is bereid en in staat voorafgaand aan elke bestelling op verzoek een drukproef voor Opdrachtgever te maken.
13. De drukproef van het repowerwerk wordt op aangeven van de Opdrachtgever door de Opdrachtnemer fysiek verstuurd aan Opdrachtgever.

14. Opdrachtnemer stemt op aangeven van Opdrachtgever de drukproef af met Opdrachtgever. Bij vragen neemt Opdrachtnemer contact op met Opdrachtgever.
15. Opdrachtnemer voert de gehele Opdracht uit nadat de drukproef door Opdrachtgever schriftelijk is goedgekeurd. Indien Opdrachtgever de drukproef afkeurt dient Opdrachtnemer haar drukproef aan te passen n.a.v. de terugkoppeling van Opdrachtgever en stuurt zij deze opnieuw fysiek aan Opdrachtgever.

## Levering

16. Leveringen worden vergezeld van een duidelijk gespecificeerde pakbon, met daarop:
  - i. objectvermelding
  - ii. bestelnummer (dit is een intern budgetnummer)
  - iii. naam en adres besteller
  - iv. aantal colli
  - v. soort en inhoud
17. Op de aan Opdrachtgever geleverde producten staat per doos aangegeven welk artikel en welk aantal het betreft.
18. Opdrachtnemer levert tijdens werkdagen, binnen de kantooruren (09.00-16.00 uur) van Opdrachtgever en stelt zich flexibel op rondom vakantieperiodes. Indien scholen gesloten zijn tijdens vakantieperiodes geeft Opdrachtgever dit aan bij Opdrachtnemer.
19. Minderleveringen worden niet geaccepteerd door de Opdrachtgever.
20. Het gewicht en de omvang van de te leveren colli voldoen aan de waarden die zijn vastgesteld in de Arbowet en regelgeving, inzake maximale gewichten en afmetingen van handmatig te vertillen verpakkingen.
21. De leveringen zijn deugdelijk verpakt. Indien er schade is aan de levering welke aantoonbaar te wijten is aan een ondeugdelijke verpakking of transport, vervangt de Opdrachtnemer de levering kosteloos.
22. Opdrachtnemer garandeert de levertermijn, kwaliteit en volledigheid zoals genoemd in de offerte-aanvraag.
23. De maximale levertijd na bestelling is twee werkdagen bij bestellingen die geplaatst zijn via de online bestelportaal.
24. Mocht Opdrachtnemer niet tijdig kunnen leveren dient Opdrachtnemer Opdrachtgever hierover direct te informeren en een oplossing met Opdrachtgever afstemmen. Opdrachtnemer zal alles in het werk stellen zo snel mogelijk te leveren in afstemming met Opdrachtgever.
25. Op verzoek van Opdrachtgever verzorgt Opdrachtnemer gepersonaliseerde mailingen aan verschillende adressen per keer. De pakketten worden door Opdrachtnemer samengesteld volgens de door Opdrachtgever opgestelde werkprocedure, geadresseerd en gefrankeerd en op de door de Opdrachtgever gewenste manier verpakt. Opdrachtnemer rapporteert hierover aan Opdrachtgever volgens de met de Opdrachtgever afgestemde richtlijnen.

## Acceptatie

26. Een door Opdrachtgever geplaatste bestelling wordt digitaal bevestigd door Opdrachtnemer middels een opdrachtbevestiging. Opdrachtnemer geeft daarbij de afname in stuks en de financiële verplichtingen aan.
27. Zo spoedig mogelijk na aflevering van het reprowerk wordt deze gecontroleerd door de eindgebruiker. Eventuele afwijkingen van de in de leveringsopdracht genoemde specificaties worden (e-mail) aan Opdrachtnemer kenbaar gemaakt. Indien de geconstateerde afwijkingen van dien aard zijn dat het geleverde niet goed bruikbaar is voor het door Opdrachtgever beoogde doel wordt het geleverde of het betreffende gedeelte afgekeurd.
28. Het afgekeurde reprowerk of het afgekeurde gedeelte wordt beschouwd als niet geleverd. Van deze afkeuring ontvangt Opdrachtnemer onmiddellijk (e-mail) bericht. Het risico en eigendom gaan van Opdrachtnemer op Opdrachtgever over op het moment van acceptatie.
29. Indien Opdrachtgever niet binnen 10 werkdagen na aflevering aan Opdrachtnemer (e-mail) heeft laten weten het reprowerk te hebben afgekeurd, wordt het als geaccepteerd beschouwd.
30. Indien reprowerk conform voorgaande procedure wordt afgekeurd dan zorgt Opdrachtnemer voor nieuw reprowerk en neemt de kosten voor eigen rekening. Binnen uiterlijk twee werkdagen vindt herlevering plaats.

## Commercieel

31. Alle prijzen zijn netto, op basis van franco levering op het aangegeven afleveradres Centrale Ontvangst Opdrachtgever, inclusief alle bijkomende kosten (zoals bijv. opslag, opstartkosten), inclusief btw.
32. Opdrachtnemer dient alle bestellingen, bevestigingen en aanvullende afspraken op schrift (digitaal) vast te leggen. Dit neemt Opdrachtnemer o.a. op in de managementrapportages die zij eenmaal per kwartaal aanlevert bij Opdrachtgever.
33. Perceel 1: Alle vervoerskosten en kosten die samenhangen met het afleveren van bestellingen zijn voor rekening van de Opdrachtnemer.
34. Perceel 2: Opdrachtnemer mag een vergoeding rekenen aan Opdrachtgever voor alle vervoerskosten en kosten die samenhangen met het afleveren van bestellingen. Hiervoor is een post opgenomen in het prijzenblad.
35. Meerleveringen worden niet betaald door Opdrachtgever.
36. Facturatie dient te geschieden volgens de factuurwijzer van Opdrachtgever: mail de factuur met bestelnummer naar [factuur@curio.nl](mailto:factuur@curio.nl).
37. Tarieven mogen éénmaal per jaar per 1 januari worden geïndexeerd. De eerste aanpassing van de tarieven mag per 1 januari 2026 plaatsvinden. Indexering vindt plaats op basis van de CBS CPI indexcijfers (Consumentenprijzen; prijsindex 2015=100, 095300 Divers drukwerk).

De maximale procentuele tariefswijziging is het percentage dat als volgt wordt berekend:  $((\text{CBS index [augustus] van het lopende jaar} - \text{CBS prijsindex index [augustus] van het voorgaande jaar}) / \text{CBS prijsindex [augustus] van het voorgaande jaar}) \times 100$ . Indien de

indexcijfers nog niet vastgesteld zijn, mogen de voorlopige cijfers gehanteerd worden zonder dat een eventuele verrekening achteraf plaatsvindt.

38. Het indexeringsvoorstel dient uiterlijk 1 maand van tevoren, dus telkens voor 1 december, schriftelijk en gespecificeerd onderbouwd ingediend te worden bij de afdeling Inkoop van Curio. Uitsluitend na schriftelijke goedkeuring van een daartoe bevoegd persoon van de afdeling Inkoop kunnen tariefswijzigingen, zowel verlagingen als verhogingen, worden doorgevoerd. Bij het niet melden van een prijsverlaging is Opdrachtnemer alsnog verplicht deze prijsverlaging met terugwerkende kracht door te voeren. Een indexeringsvoorstel dat na 1 december wordt ingediend mag niet per 1 januari worden doorgevoerd. Vanaf de ingediende datum dient er één volle kalendermaand tussen indienen en doorvoeren te zitten.
39. Opdrachtnemer verstuurt per Opdracht een digitale factuur welke minimaal voorzien is van de volgende gegevens:
  - i. bestelnummer
  - ii. Naam besteller
  - iii. Factuuradres
  - iv. Factuurdatum
  - v. Afleveradres
  - vi. Omschrijving van het geleverde reproductie
  - vii. Objectvermelding
  - viii. Oplage
  - ix. Druk
  - x. Afgewerkt format
  - xi. Proef
  - xii. Papier
  - xiii. Afwerking

## Privacy en security

40. Medewerkers van Opdrachtnemer zijn gebonden aan geheimhoudingsverklaringen ten aanzien van alle data van Opdrachtgever. Deze geheimhoudingsverklaringen worden na gunning besproken met Opdrachtnemer.
41. Opdrachtnemer zorgt voor gepaste bewustwording en kennis van informatiebeveiliging onder medewerkers van Opdrachtnemer.
42. Opdrachtnemer conformeert zich aan de volgende richtlijnen:

| Richtlijn                                       | Toelichting                                                                                                                                                                                                                                                                 | Eis                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Verificatie                                                                                                                                                                                                                                                                         |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NCSC adviezen</b>                            | Een beveiligingsadvies wordt door het NCSC gepubliceerd naar aanleiding van een recent gevonden kwetsbaarheid of geconstateerde dreiging. In een beveiligingsadvies staat de beschrijving, de mogelijke gevolgen en mogelijke oplossingen van de kwetsbaarheid of dreiging. | Op het moment dat een kwetsbaarheid (beveiligingsadvies) wordt gepubliceerd door de geldende formele organen (thans NCSC) zie: <a href="https://www.ncsc.nl/actueel/beveiligingsadviezen">https://www.ncsc.nl/actueel/beveiligingsadviezen</a> dan hanteert opdrachtnemer een methode om hierop te acteren als de kwetsbaarheid onderdeel uitmaakt van de website, online middelen of de onderliggende resources.                                                        | Akkoordverklaring door de opdrachtgever met toelichting hoe wordt geborgd dat de beveiligingsadviezen worden opgevolgd en hoe Curio hierover wordt geïnformeerd.                                                                                                                    |
| ICT beveiligingsrichtlijnen voor webapplicaties | De ICT beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC) zijn criteria voor het veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur.                                                     | De opdrachtnemer draagt zorg dat het online middel voldoet aan de richtlijnen ICT beveiligingsrichtlijnen voor webapplicaties en toont dat aan. Zie: <a href="https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties">https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties</a>                                                                                         | De opdrachtgever verricht na oplevering een acceptatietest om te beoordelen of voor het online middel daadwerkelijk deze beveiligingsmaatregelen zijn genomen.                                                                                                                      |
| <b>CVSS</b>                                     | Het Common Vulnerability Scoring System is een open industriestandaard voor het beoordelen van de ernst van beveiligingsproblemen in computersystemen.                                                                                                                      | Er zijn geen kwetsbaarheden actief op de website of online middelen (en alle onderliggende resources) met een CVSS-score hoger dan 6.9 (Hoog/Kritiek).<br><br><b>N.B.:</b> Wanneer er persoonsgevoelige data betrokken is, of het bedrijfsrisico hoog is, dan is een onafhankelijk pentest door een door Curio aangewezen Ethical Hacker verplicht.                                                                                                                      | 1. Akkoordverklaring door de opdrachtgever met toelichting hoe wordt geborgd dat het online middel blijvend aan de standaard voldoet.<br>2. Opdrachtgever stemt met de CISO af of een onafhankelijke pentest nodig is om de CVSS-scores van de betrokken componenten te verifiëren. |
| <b>OWASP</b>                                    | De OWASP een standaard bewustwordingsdocument voor ontwikkelaars en webapplicatiebeveiliging. Het vertegenwoordigt een brede consensus over de meest kritieke beveiligingsrisico's voor webapplicaties.                                                                     | Voor aan Internet gekoppelde ICT systemen gelden minimaal de Open Web Application Security Project (OWASP) criteria. Voor nieuwe ICT systemen, upgrades en nieuwe versies wordt, voorafgaand aan de acceptatie, een test van het systeem uitgevoerd tegen vooraf opgestelde acceptatiecriteria, waarbij ook de top 10 kwetsbaarheden worden gecontroleerd. Van deze test wordt een testrapport opgesteld. Zie ook: <a href="https://owasp.org/">https://owasp.org/</a> . | Akkoordverklaring door de opdrachtgever met toelichting hoe wordt geborgd dat het online middel blijvend aan de standaard voldoet.                                                                                                                                                  |

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                        |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>STITCH</b>                                          | Opdrachtnemer zorgt er in aanvulling op de OWASP richtlijnen voor dat het de principes opgesteld door brancheorganisatie SURF implementeert inclusief bijbehorende eisen en implicaties, gedurende de looptijd van de overeenkomst.                                                                                                                                                                                   | Security Technical IT Checklist Zie: <a href="https://www.surf.nl/en/stitch-a-short-checklist-for-application-security">https://www.surf.nl/en/stitch-a-short-checklist-for-application-security</a>                                                                                                                                                                                                            | Akkoordverklaring door de opdrachtgever met toelichting hoe wordt geborgd dat het online middel blijvend aan de standaard voldoet.                                                                     |
| <b>HTTPS, TLS &amp; certificaten</b>                   | HTTPS (Hyper Text Transfer Protocol Secure) verschijnt in de URL wanneer een website is beveiligd met een TLS certificaat. TLS staat voor Transport Layer Security. TLS zorgt ervoor dat de data die verstuurd wordt tussen de gebruiker en de website of tussen systemen onderling wordt versleuteld en zo onleesbaar wordt gemaakt.                                                                                 | De opdrachtnemer biedt op het online middel volledig werkende ondersteuning voor beveiligde verbindingen conform TLS. Dit betekent dat er een geldig certificaat is geïnstalleerd op het online middel op basis waarvan andere systemen een TLS-verbinding kunnen opzetten met het online middel en waarvan de veiligheid van de TLS-configuratie voldoet aan de ICT-beveiligingsrichtlijnen voor TLS van NCSC. | De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de web- en mailtest op <a href="http://www.internet.nl">www.internet.nl</a> |
| <b>Domain Name System Security Extensions (DNSsec)</b> | DNSsec is een uitbreiding op het Domain Name System (DNS). Het verhelpt een aantal kwetsbaarheden in DNS. Hierdoor wordt de 'bewegwijzering' van het internet veiliger en vertrouwder.                                                                                                                                                                                                                                | De opdrachtnemer biedt op het online middel volledig werkende ondersteuning voor DNSsec. Domeinnaam-informatie, zoals bijbehorende IP-adressen, zijn met een geldige DNSsec-handtekening ondertekend.                                                                                                                                                                                                           | De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de web- en mailtest op <a href="http://www.internet.nl">www.internet.nl</a> |
| <b>Toegankelijkheid (EN301549 en WCAG2.1)</b>          | EN301549 is een Europese toegankelijkheidsstandaard die omschrijft aan welke eisen een (web) toepassing moet voldoen om toegankelijk te zijn voor mensen met een functiebeperking. Voor webcontent verwijst EN301549 naar een andere internationale standaard: WCAG 2.1 van het World Wide Web consortium (W3C).                                                                                                      | De opdrachtnemer zorgt ervoor dat het online middel minimaal voldoet aan de open standaard Toegankelijkheid (WCAG2.0).                                                                                                                                                                                                                                                                                          | De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit aan deze eis, bijv. op paginaniveau met Achecker of op siteniveau met Powermapper                                        |
| <b>Internet Protocol versie 6 (IPv6)</b>               | Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen systemen binnen een netwerk, zoals internet, mogelijk. De standaard bepaalt dat ieder systeem binnen het netwerk een uniek nummer (IP-adres) heeft. De belangrijkste motivatie voor de ontwikkeling van IPv6 was het vergroten van de hoeveelheid beschikbare adressen ten opzichte van de voorganger IPv4.                                      | De opdrachtnemer biedt op het online middel volledig werkende ondersteuning voor IPv4 én IPv6 (dual stack). Dit betekent in ieder geval dat gebruikers online middelen kunnen bezoeken, e-mail kunnen verzenden en ontvangen, en andere systemen kunnen bereiken via IPv4 en via IPv6 zonder dat er sprake is van functionele of non-functionele (bijv. qua prestatie) verschillen.                             | De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de web- en mailtest op <a href="http://www.internet.nl">www.internet.nl</a> |
| <b>Security Assertion Markup Language (SAML)</b>       | De Security Assertion Markup Language (SAML), is een XML-gebaseerd raamwerk voor het communiceren van gebruikers authenticatie, rechten, en attributen informatie. SAML biedt organisatie entiteiten de mogelijkheid om claims te maken over de identiteit, attributen en rechten van een subject (een entiteit welke vaak een menselijke gebruiker is) aan andere entiteiten zoals Internet applicaties of diensten. | De opdrachtnemer biedt bij toepassen van een inlog op het online middel volledig werkende ondersteuning voor SAML versie 2.0, zodat gebruikers via eenmalig in- en uitloggen veilige toegang hebben tot verschillende gekoppelde webdiensten. Daarbij hoort het succesvol doorlopen en aantonen van Interoperability Certification Program van Kantara of vergelijkbaar.                                        | De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit aan deze eis.                                                                                                            |

|                   |                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                  |                                                                                                              |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Domeinnaam</b> | Voor domeinnamen van Curio bestaan afspraken. Deze zorgen voor eenduidigheid, transparantie, kostenbeheersing en bescherming van de juridische positie. De Dienst IT is registrar en houder van alle domeinnamen van Curio. De vindbaarheid van het domein kan worden bevorderd door SEO en eventueel SEA. | Er wordt een domeinnaam geclaimd dat voldoet aan het Curio beleid. De voorkeur heeft een subdomein van @curio.nl. Afhankelijk van de doelgroep wordt er een losstaand nieuw .nl, .eu of .com domein geclaimd, dat eventueel via een redirect alsnog naar een @curio.nl-domein wordt doorgelinkt. | De opdrachtgever vraagt via de IT-liaison van Curio een domeinnaam aan die voldoet aan het domeinnaambeleid. |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|

Aanvullend in geval van het toepassen van mail op het online middel gelden aanvullend onderstaande eisen. Als er geen mailfunctie wordt gebruikt, dan wordt op het domein de mailfunctionaliteit uitgeschakeld (no\_mail).

| Richtlijn                                 | Toelichting                                                                                                                                                                                                                                                                      | Eis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Verificatie                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DMARC</b>                              | DMARC is een standaard voor het veiliger maken van e-mail verkeer door het tegengaan van spam en phishing door misbruik van domeinnamen bij e-mail te voorkomen. Deze richtlijn geldt voor uitgaande en inkomende e-mail en in domeinnaamsystemen (DNS).                         | De opdrachtnemer biedt <b>bij toepassen van mail</b> op het online middel volledig werkende ondersteuning voor DMARC.                                                                                                                                                                                                                                                                                                                                                                                                                                                         | De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de mailtest op <a href="http://www.internet.nl">www.internet.nl</a>                                                                                                                        |
| <b>Domain Keys Identified Mail (DKIM)</b> | DKIM koppelt e-mail aan een domeinnaam met behulp van een digitale handtekening. Hierdoor kan de ontvanger zien welke domeinnaam en achterliggende organisatie verantwoordelijk is voor het zenden van de e-mail. Spam- en phishingmails kunnen daardoor beter worden gefilterd. | De opdrachtnemer biedt <b>bij toepassen van mail</b> op het online middel volledig werkende ondersteuning voor DKIM. Dit betekent dat op het systeem een publiek/privaat sleutelpaar is gegenereerd en dat de publieke DKIM-sleutel is gepubliceerd in de DNS van de e-maildomeinnaam en dat alle uitgaande e-mailberichten worden ondertekend met de private DKIM-sleutel en dat alle inkomende e-mailberichten worden gecontroleerd op de geldigheid van een eventuele DKIM- handtekening en het systeem hieraan mogelijke acties verbindt, welke met Curio zijn afgestemd. | De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de mailtest op <a href="http://www.internet.nl">www.internet.nl</a><br><br>Als er geen mailfunctie wordt gebruikt, dan wordt op het domein de mailfunctionaliteit uitgeschakeld (no_mail). |
| <b>Sender Policy Framework (SPF)</b>      | Sender Policy Framework (afgekort SPF) is een protocol dat tot doel heeft te helpen spam te verminderen, door vast te stellen of de verzender van een mailbericht gerechtigd is om een bericht te verzenden namens de afzender van het bericht.                                  | De opdrachtnemer <b>biedt bij toepassen van mail</b> op het online middel volledig werkende ondersteuning voor SPF. Dit betekent dat IP-adressen van de verzendende systemen als SPF-record worden geregistreerd in de DNS van de verzendende domeinnaam. Alle inkomende e-mailberichten worden gecontroleerd op de geldigheid van het verzendend IP-adres tegen het IP-adres dat in SPF-record staat van de verzendende domeinnaam.                                                                                                                                          | De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de mailtest op <a href="http://www.internet.nl">www.internet.nl</a><br><br>Als er geen mailfunctie wordt gebruikt, dan wordt op het domein de mailfunctionaliteit uitgeschakeld (no_mail). |



|                         |                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>STARTTLS en DANE</b> | STARTTLS in combinatie met DANE gaan het af luisteren of manipuleren van mailverkeer tegen. STARTTLS maakt het mogelijk om transportverbindingen tussen e-mailservers op basis van certificaten met TLS te beveiligen. Met de complementaire standaard DANE kunnen e-mailservers het gebruik van TLS bovendien afdwingen. | De opdrachtnemer biedt <b>bij toepassen van mail</b> op het online middel volledig werkende ondersteuning voor STARTTLS (SMTP over STARTTLS, oftewel ESMTS) in combinatie met DANE. Verzendende mailservers kunnen daarmee een versleutelde verbinding over een onvertrouwd netwerk (zoals internet) opzetten. Dit voorkomt dat aanvallers het mailverkeer kunnen af luisteren (passieve aanvallers) en/of kunnen manipuleren (actieve aanvallers). | De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, met minimaal een 100% score op de mailtest op <a href="http://www.internet.nl">www.internet.nl</a><br><br>Als er geen mailfunctie wordt gebruikt, dan wordt op het domein de mailfunctionaliteit uitgeschakeld (no_mail). |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### 43. Opdrachtnemer conformeert zich aan de volgende wettelijke vereisten:

| Wet                                             | Toelichting                                                                                                                                                                                                       | Eis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Verificatie                                                                                                                                                                                                                     |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Telecommunicatiewet (Cookiewet)</b>          | Volgens de cookiebepaling in de Telecommunicatiewet moet de website haar bezoekers informeren en toestemming krijgen voor het gebruik van cookies. Dit geldt ook voor andere methodes van informatie wegschrijven | De opdrachtnemer biedt op het online middel volledig werkende ondersteuning voor functionele/ webanalyse cookies die voldoen aan de Telecommunicatiewet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | De opdrachtgever toetst na opleveren en minimaal per kwartaal de conformiteit van deze eis, bijv. met de Ghostery plugin of app. Er dient geen gebruik te worden gemaakt van third party cookies, enkel van webanalyse cookies. |
| <b>Algemene Verordening Gegevensbescherming</b> | Curio is verplicht om persoonsgegevens goed te beschermen. En ze alleen te verwerken als we daar een goede reden voor hebben.                                                                                     | De opdrachtgever dient bij toepassen van persoonsgegevens op het online middel te garanderen dat het online middel en opdrachtgever voldoet aan de vereisten van de Algemene Verordening Gegevensbescherming. De opdrachtgever bepaalt de classificatie van persoonsgegevens en bepaalt wat passende technische- en organisatorische maatregelen zijn. De opdrachtnemer neemt deze passende maatregelen ter bescherming van de persoonsgegevens. De opdrachtgever sluit met de opdrachtnemer een verwerkersovereenkomst af <b>(conform de standaard van Curio)</b> waarbij afspraken worden gemaakt over de verantwoording bijv. mogen uitvoeren van audits bij de opdrachtnemer, TPM verklaring. De opdrachtgever blijft verantwoordelijk voor de naleving van de AVG en dient maatregelen te nemen zoals opname in AVG register of het verrichten van een DPIA. | De opdrachtgever heeft met de opdrachtnemer een verwerkersovereenkomst afgesloten (zie bijlage: 'Verwerkersovereenkomst') en er is door opdrachtgever een DPIA op het online middel uitgevoerd.                                 |

44. De Opdrachtnemer heeft processen en services in place die in overeenstemming zijn met en voldoet aan de principes van privacy en security by design.

45. De Opdrachtnemer beschikt over een datalekprocedure waarbij klant tijdig op de hoogte wordt gebracht van een privacy-incident via <https://www.curio.nl/datalek>.



46. Opdrachtnemer verwerkt persoonsgegevens alleen op basis van schriftelijke instructies van Curio. Persoonsgegevens worden niet gebruikt voor eigen doeleinden en ook niet verkocht. Als een sub-verwerker toegang heeft tot persoonsgegevens dan worden daaromtrent afspraken gemaakt in overeenstemming met de afspraken in de verwerkersovereenkomst.
47. Alleen de Opdrachtnemer en Opdrachtgever hebben toegang tot de data. Ook is het mogelijk om functiescheiding te gebruiken: niet iedere rol kan alles zien of doen.
48. De opslag en verwerking van persoonsgegevens door Opdrachtnemer geschiedt binnen de EER.
49. Bij gebruik van de dienst wordt door Opdrachtnemer niet meer persoonsgegevens verzameld en opgeslagen dan noodzakelijk voor het doeleinde van de verwerking.
50. Het is voor Opdrachtgever mogelijk met behulp van een eigen interface de data van een specifieke natuurlijke persoon snel en eenvoudig te verwijderen. Indien relevant kan een deel van de data verwijderd worden.
51. Wanneer daar aanleiding toe is kunnen persoonsgegevens worden aangepast door Opdrachtgever.
52. Bewaartermijnen worden bepaald door Curio als verwerkingsverantwoordelijke. Persoonsgegevens worden niet langer opgeslagen dan noodzakelijk.
53. Een verzoek om inzage van de persoonlijke data van een data subject kan snel en door Opdrachtgever zelf uitgevoerd worden, dan wel Opdrachtnemer beschikt over processen om Opdrachtgever daarbij te assisteren.
54. Opdrachtnemer garandeert dat Onderaannemers van Opdrachtnemer die relevant zijn voor het leveren van het systeem aan dezelfde beveiligings- en privacy eisen voldoen

## **Duurzaamheid**

55. Papier dient minimaal van 100% FSC materiaal van hout uit goed beheerde bossen te zijn. Aanvullend dient binnen 2 jaar minimaal 75% van het papier van gerecycled materiaal zijn met een zo'n hoog mogelijk recyclepercentage (100% waar mogelijk).
56. Opdrachtnemer biedt verschillende soorten duurzaam papier aan. Denk hierbij aan groeipapier, ongebleekt en gerecycled papier.
57. Er dient zo min mogelijk verpakkingsmateriaal aanwezig te zijn/gebruikt te worden. Indien dit toch benodigd is, dan dient het verpakkingsmateriaal zoveel mogelijk van gerecycled materiaal te zijn gemaakt en zoveel mogelijk te scheiden zijn in onderdelen van één materiaal of dient te worden hergebruikt door opdrachtnemer.
58. Het gebruik van schadelijke stoffen dient zoveel mogelijk vermeden te worden. Zeer Zorgwekkende Stoffen mogen niet gebruikt worden.
59. De gehele opdracht wordt door Opdrachtnemer zoveel mogelijk plastic vrij uitgevoerd.
60. Voor al deze duurzaamheidseisen geldt dat op verzoek van Opdrachtgever de rapporten/documentatie overlegd wordt door Opdrachtnemer waaruit blijkt dat aan de genoemde criteria is voldaan.

## 11. Koppeling

61. Opdrachtnemer zorgt kosteloos voor een OCI-koppeling tussen haar bestelportaal en het purchase-to-pay systeem van Opdrachtgever (Afas).