Toelichting Programma van Eisen

Programma van Eisen - Toelichting

V 4.0 14-10-2024

yonder

Documenthistorie

Versie	Datum	Door	Toelichting
1.0	19-04-2021	J. de Bruijn	Publicatieversie
2.0	29-08-2022	J. Kolen	Wijzigingen ivm - Modellen verwerkersovereenkomst 4.0 (voorheen versie 3.0) - MBO Digitaal (voorheen saMBO-ICT) - Certificeringsschema 3.0 (voorheen versie 2.0)
3.0	04-10-2024	E. vd Breevaart	Aanvullingen: - Richtlijnen certificaten (39) Wijziging: - Emailen namens opdrachtgever (30) Re-styling op basis van Yonder template
4.0	14-10-2024	J. Kolen	Tekstuele wijziging Onderwijsgroep Tilburg in Yonder

Inhoud

1 Inleiding

Dit document beschrijft de inkoop van een applicatie door Yonder. Bij inkoop van een applicatie wordt getoetst of deze voldoet aan het door Yonder gehanteerde Programma van Eisen. In dit document wordt een toelichting op de afzonderlijke eisen uit het Programma van Eisen gegeven.

Bij de inkoop van een applicatie e.d. wordt door Yonder gewerkt met een inkoopovereenkomst en de algemene voorwaarden van Yonder zijn daarbij van toepassing. Om de contractuele afspraken vast te leggen wordt gewerkt met een standaard inkoopovereenkomst (leverings- en/of dienstenovereenkomst). De inkoopovereenkomst wordt voor akkoord aan de leverancier voorgelegd. Daarbij worden de Algemene voorwaarden voor Leveringen en Diensten Yonder - 2021 gehanteerd. De algemene voorwaarden zijn te raadplegen op de website van Yonder. Hiervoor verwijzen we naar: Voorwaarden | Yonder

Op het moment dat er persoonsgegevens worden verwerkt in de applicatie wordt ook een verwerkersovereenkomst gesloten. Yonder maakt gebruik van twee modellen verwerkersovereenkomst en gaat niet akkoord met andere verwerkersovereenkomsten. Het betreft het model verwerkersovereenkomst 4.0 behorende bij het Privacy Convenant en de algemene model verwerkersovereenkomst 4.0 behorende tot het IBP Framework van MBO Digitaal. Binnen de onderwijssector is overeengekomen dat de betreffende modellen worden gebruikt en inhoudelijk niet worden gewijzigd. Hiervoor verwijzen we naar:

- Privacyconvenant
- Framework IBP - MBO Digitaal

Opdrachtnemer dient akkoord te gaan met het gebruik van één van de genoemde modellen en dient bij het aangaan van de inkoopovereenkomst bijlagen 1 en 2 van deze modellen in te vullen. Uit bijlage 1 moet voldoende duidelijk worden welke persoonsgegevens worden verwerkt. In bijlage 2 moet de verwerker verklaren of aan de minimale beveiligingsnormen wordt voldaan. De ingevulde bijlagen 1 en 2 worden door de Coördinator Informatiebeveiliging en Functionaris Gegevensbescherming getoetst en beoordeeld. Binnen Yonder worden de inkoopovereenkomst en verwerkersovereenkomst gelijktijdig door het College van Bestuur ondertekend. Beide overeenkomsten zijn onlosmakelijk met elkaar verbonden.

De daadwerkelijk afgesloten overeenkomst en verwerkersovereenkomst zijn bovenliggend ten opzichte van dit document. Verder zijn de algemene inkoopvoorwaarden van Yonder van toepassing. De regie van het inkooptraject ligt binnen Yonder bij Inkoop. De contacten met de opdrachtnemer over de inkoopovereenkomst, verwerkersovereenkomst, Programma van Eisen en aanvullende documenten lopen via Inkoop.

2 Toelichting

Sinds eind 2019 gebruikt Yonder een standaard lijst met eisen bij de inkoop van applicaties. Deze betreffen niet zozeer functionele eisen als wel technische, informatiebeveiligings- en wettelijke vereisten. Dit programma van eisen wordt als referentie gebruikt, zodat elk inkooptraject met een ict component tegen dezelfde eisen getoetst worden. Niet elke eis is overigens van toepassing op elk inkooptraject, dit wordt aan het begin ervan vastgesteld.

Aangezien de eisen zelf kort geformuleerd zijn volgt hieronder steeds de eis en een toelichting.

3 Algemeen

1	**De applicatie wordt als "Software as a service" oplossing geleverd.**
Toelichting	Opdrachtgever hoeft geen (server-)applicatie(s) te installeren en/of te configureren. De applicatie werkt volledig via de browser. Op andere mobiele devices kan eventueel een app gebruikt worden.

4 Wettelijke kaders

2	**De applicatie voldoet gedurende de looptijd van de overeenkomst aan de relevante geldende wet- en regelgeving, zonder dat hiervoor additionele kosten in rekening worden gebracht aan de opdrachtgever.**
Toelichting	In deze eis gaat om het blijvend voldoen aan de relevante wet- en regelgeving. Ook bij wijziging van wet- en regelgeving gedurende de looptijd van de overeenkomst, dient aan de dan geldende wet- en regelgeving te worden voldaan. Als het proces of de gegevensverwerking als gevolg van gewijzigde wet- en regelgeving verandert, dan zal de benodigde functionaliteit in de applicatie ontwikkeld of aangepast worden en tijdig beschikbaar zijn. Hiervoor worden door opdrachtnemer geen additionele kosten in rekening gebracht.

3	**De applicatie voldoet aan de eisen van de onderwijssectoren voor het voortgezet onderwijs (VO) en/of middelbaar beroepsonderwijs (MBO) waaronder de Aanpak IBP van Kennisnet, het Framework IBP van MBO Digitaal, en de aanbevelingen van de relevante gebruikersgroepen en de relevante standaarden van overheidsinstellingen.**
Toelichting	Naast de geldende wet- en regelgeving (zoals genoemd in eis 2) zijn er aanvullende eisen vanuit de onderwijssectoren (VO en MBO). Opdrachtnemer voldoet aan deze eisen en kan hierover nadere informatie bij opdrachtgever opvragen. Indien de eisen en/of richtlijnen veranderen, zal de benodigde functionaliteit in de applicatie ontwikkeld of aangepast worden en tijdig beschikbaar zijn. Hiervoor worden door opdrachtnemer geen additionele kosten in rekening gebracht. Bron: Framework IBP - MBO Digitaal en Aanpak IBP in het onderwijs - Kennisnet

4	**De opdrachtnemer verleent medewerking aan het uitvoeren van een "BIV-classificatie" en "DPIA" om te kunnen beoordelen welke beveiligingseisen en -maatregelen van toepassing zijn.**
Toelichting	De AVG gaat er vanuit dat opdrachtgever de (persoons)gegevens classificeert op de benodigde Beschikbaarheid, Integriteit en Vertrouwelijkheid. Vervolgens is opdrachtgever verplicht een Data Protection Impact Assessment (DPIA) te doen. Voor deze risico inschatting en het treffen van passende maatregelen is samenwerking met en medewerking van de opdrachtnemer noodzakelijk.

5 Inkoop- en contractvoorwaarden

5	**Alle data mag uitsluitend worden verwerkt voor de doeleinden overeengekomen met de opdrachtgever.**
Toelichting	Aangezien een opdrachtnemer namens opdrachtgever persoonsgegevens verwerkt, is het niet de bedoeling dat deze eigenhandig door de opdrachtnemer verkocht of op welke andere wijze dan ook gedeeld wordt met derden, dan wel door opdrachtnemer zelf voor andere doeleinden worden gebruikt. Wel kan een opdrachtnemer voor de overeengekomen doeleinden gebruik maken van een subverwerker(s). Deze subverwerker dient bekend te zijn. Een subverwerker mag de persoonsgegevens ook niet gebruiken voor andere doeleinden dan bedoeld in de opdracht.

6	**De opdrachtnemer staat toe dat alle door opdrachtgever aangemerkte data op verzoek als archief gedownload kan worden in een door de opdrachtgever te bepalen gangbaar formaat.**
Toelichting	Voor continuïteit wil opdrachtgever zelf de beschikking hebben over de data. Voorbeelden van gangbare formaten zijn sql, xlsx, json of csv.

7	**Op verzoek of na instemming van de opdrachtgever staat de opdrachtnemer exporteren van data toe naar een andere cloud provider binnen 5 werkdagen.**
Toelichting	Deze eis is relevant als de benodigde storage erg groot is, bijvoorbeeld bij mediabestanden. Hiermee wordt het mogelijk gemaakt om de opslag rechtstreeks te verplaatsen zonder lange wachttijden voor down- en upload.

8	**De opdrachtnemer verwijdert alle gegevens op verzoek van de opdrachtgever binnen de door opdrachtgever gestelde termijn en kan dit ook aantonen.**
Toelichting	Als de applicatie niet meer gebruikt wordt of de overeenkomst wordt beëindigd moeten de gegevens van opdrachtgever aantoonbaar (met behulp van logging bijvoorbeeld) verwijderd worden.

9	**Bij het verwijderen van gegevens (zoals hierboven) wordt door de opdrachtnemer gegarandeerd dat de betreffende gegevens onder andere uit, maar niet beperkt tot, de back-ups worden verwijderd.**
Toelichting	Gegevens moeten bij verwijdering overal verwijderd worden. Bijvoorbeeld uit de backups en eventuele test-, cursus- en acceptatieomgevingen.

10	**De opdrachtnemer beschikt over een SAAS-Escrow voorziening**
Toelichting	Dit houdt in dat de continuïteit van de dienst, ingeval van faillissement van de Opdrachtnemer of één van haar onderaannemers (bijvoorbeeld de hostingpartij) door middel van een onderliggende contractuele bepaling is geborgd. Denk hierbij aan een voorziening die ervoor zorgdraagt dat de hostingdienst x maanden wordt gefinancierd.

6 Algemene Basisvoorziening

11	**Medewerkers van de opdrachtnemer, die in contact treden met Yonder beheersen de Nederlandse taal in gesproken woord en schrift.**
Toelichting	De voertaal binnen opdrachtgever is Nederlands. Opdrachtnemer sluit hierop aan ten behoeve van de communicatie. Wel kan bij internationale opdrachtnemers de supportdesk in het Engels zijn. Communicatie door de opdrachtnemer met de eindgebruikers vindt in het Nederlands plaats.

12	**Elke vorm van zichtbare communicatie en documentatie zoals, maar niet beperkt tot, schermen, rapporten en gebruikershandleidingen van de applicatie, zijn in de Nederlandse taal.**
Toelichting	Documentatie van de opdrachtnemer voor de eindgebruikers is in het Nederlands.

7 SAAS-Omgeving

13	**Onderhoud en ondersteuning op de applicatie is gegarandeerd gedurende de gehele looptijd van de overeenkomst. Dit is vastgelegd in een SLA, waarbij de applicatie wordt aangeboden op minimaal de één na laatste major-release (n-1).**
Toelichting	De opdrachtnemer neemt de ontwikkeling van de applicatie op zich en support deze. Tijdens de looptijd van de overeenkomst worden updates en upgrades uitgerold. Opdrachtgever blijft niet achter in versies (afgezien van beta of testversies) en er worden geen additionele kosten voor in rekening gebracht.

14	**De applicatie ondersteunt gedurende de looptijd van de overeenkomst clients op alle door Microsoft ondersteunde operating systemen**
Toelichting	In de praktijk komt dit neer op browsers die werken op Windows10 op een laptop of PC.

15	**De opdrachtnemer doet zelf de hosting, ontwikkeling en het technisch beheer.**
Toelichting	Opdrachtgever hoeft niets te installeren, configureren of te onderhouden in het eigen datacenter. De kosten van hosting, ontwikkeling en technisch beheer maken onderdeel uit van de SaaS-gebruikskosten.

16	**De applicatie moet HTML5 compatible zijn en werken op minimaal de één na laatste major-release (n-1) van de 3 meest gangbare internetbrowsers gedurende de gehele looptijd van de overeenkomst.**
Toelichting	Die onderdelen van de applicatie die werken via een browser moeten blijven werken bij de nieuwere versies daarvan. Er is dus geen oude browserversie vereist om te kunnen werken. Als er onderdelen werken via een app (Android of iOS) dan is dat zeker prima. Mits deze apps geüpdatet worden om te blijven werken op de laatste en de één na laatste major-release van Android of iOS.

17	**De applicatie moet zich aanpassen aan de verschillende devices en 'responsive' pagina's genereren of, na akkoord van de opdrachtgever, een app aanbieden.**
Toelichting	Webpagina's die responsive zijn, verplaatsen de inhoud naast of juist onder elkaar afhankelijk van het device, om te voorkomen dat horizontaal scrollen nodig is.

18	**Voor de werking van de applicatie heeft een eindgebruiker geen propietary technieken nodig waaronder, maar niet beperkt tot, Flash, Silverlight, .net (wpf) of Java-applicaties.**
Toelichting	Het doel van deze eis is vooral het voorkomen van de noodzaak van plugins of extensies in browsers.

19	**De applicatie ondersteunt zowel het IPv4 als het IPv6 protocol.**
Toelichting	Op dit moment is de infrastructuur van Yonder gebaseerd op IPv4.De infrastructuur zal op een nog nader te bepalen moment worden gemigreerd naar het IPv6 protocol in verband met de schaarste aan IPv4 adressen. Daarnaast kunnen er op dit moment al (thuis-)werkplekken zijn, die gebruik maken van het IPv6 protocol. De opdrachtnemer dient daarom zowel het IPv4 als het IPv6 protocol te ondersteunen.

20	**De opdrachtgever bepaalt of de applicatie volledig dient te functioneren op een door opdrachtgever te bepalen domeinnaam.**
Toelichting	Afhankelijk van de doelgroep waarop de clouddienst is gericht, kan opdrachtgever verlangen dat de applicatie volledig dient te functioneren op een door de opdrachtgever te bepalen domeinnaam.

21	**Updates en upgrades kunnen in productie worden uitgerold en er zijn daarvoor geen service windows nodig (continuous delivery)**
Toelichting	Doel van deze wens is een hoge beschikbaarheid van het systeem doordat deze incrementeel onderhouden kan worden.

8 Identity & Security

Onderstaande eisen gaan dieper in op de manier waarop onze gebruikers zich bekend maken bij het systeem van de opdrachtnemer en welke toegang zij daarmee krijgen. De eisen behandelen manieren om kenbaar te maken WIE iemand is (identificatie), dat dit klopt (authenticatie) en WAT deze persoon dan mag (autorisatie).

22	**Voor het inloggen wordt aangesloten op SURFconext.**
Toelichting	SURFConext is een op SAML/OpenID gebaseerde federatie en geldt als de de facto standaard binnen het MBO, HO en WO. Het maakt veilig, gemakkelijk en privacy vriendelijke authenticatie en autorisatie mogelijk. Met één set credentials kan een gebruiker (SSO) inloggen op een groot aantal (cloud)diensten. Door gebruik te maken van SURFconext kan overal de door Yonder gehanteerde inlog worden toegepast. Opdrachtnemer beschikt hiermee dan ook niet zelf over de wachtwoorden van onze medewerkers en deelnemers. Meer informatie over SURFconext in het algemeen: https://surf.nl/surfconext Technische informatie over SURFconext: https://wiki.surfnet.nl/display/surfconextdev/Documentation+for+Service+Providers Kennisnet is een op SAML/OpenID gebaseerde federatie en geldt als de de facto standaard binnen het VO. Het maakt veilig, gemakkelijk en privacy vriendelijke authenticatie en autorisatie mogelijk.

23	**De opdrachtnemer sluit voor two factor authenticatie (2FA) aan bij het het SURFsecureID platform.**
Toelichting	Opdrachtnemer hoeft zelf geen 2FA te leveren, maar dit wordt afgehandeld door SURFsecureID op het SURFconext platform. Wel is het nodig dat het systeem van de opdrachtnemer dit kan initiëren middels Levels of Assurance (LoA). Opdrachtnemer regelt dit in op verzoek van opdrachtgever. Opdrachtgever zal daarbij aangeven wat de sessieduur (geldigheidsduur token) moet zijn. Meer informatie over SURFsecureID in het algemeen: https://surf.nl/surfsecureid Technische informatie over LoA binnen SURFsecureID: https://wiki.surfnet.nl/display/SsID/Using+Levels+of+Assurance+to+express+strength+of+authentication

24	**De applicatie ondersteunt Step Up authentication op het SURF SecureID platform voor specifieke, configureerbare rollen.**
Toelichting	Het is de bedoeling om rollen met een laag risicoprofiel, met de applicatie te laten werken zonder 2FA en voor rollen die krachtigere functionaliteiten nodig hebben of met vertrouwelijke gegevens werken wel 2FA in te zetten.

25	De applicatie ondersteunt Step Up authentication op het SURF SecureID platform voor specifieke, configureerbare schermen?
Toelichting	Het betreft hier gegevens met Vertrouwelijkheid is Hoog uit de BIV-classificatie, die alleen zichtbaar mogen zijn voor specifieke rollen, terwijl de overige onderdelen van het scherm ook bij andere rollen open moet kunnen staan. Alternatief is dat elk scherm of functionaliteit afgebakend is tot gebruik binnen één rol. Het effect is dat voor het uitvoeren van eenvoudige taken met een laag risico het gebruik van de app laagdrempelig blijft.

26	De applicatie biedt een provisioning koppelvlak.
Toelichting	Door middel van een API biedt de SAAS-applicatie de mogelijkheid om accounts en rollen te preprovisionen. Surfconext biedt provisioning 'on demand'. De gebruiker hoeft dan niet vooraf bekend te zijn maar wordt aangemaakt bij de eerste inlog. (Dit kan zijn op basis van SurfConext attributen). Indien preprovisioning noodzakelijk is, wordt aangesloten op het RedSpider platform voor het uitwisselen van aanvullende identiteitsattributen. De opdrachtnemer is verantwoordelijk voor het ophalen van de benodigde attributen.

27	De applicatie biedt een deprovisioning koppelvlak.
Toelichting	Door middel van een API biedt de SAAS-applicatie de mogelijkheid om accounts en rollen te deactiveren of te verwijderen, afhankelijk van attributen. Indien deprovisioning noodzakelijk is, wordt aangesloten op het RedSpider platform voor het uitwisselen van aanvullende identiteitsattributen. De opdrachtnemer is verantwoordelijk voor het ophalen van de benodigde attributen.

28	De applicatie biedt een federatief koppelvlak aan voor uitwisseling van rollen.
Toelichting	Rollen die gedefinieerd zijn in de kernsystemen van opdrachtgever kunnen automatisch worden doorgezet naar andere applicaties. Deze rollen kunnen gekoppeld worden aan autorisatiematrixen voor verdere toegang.

29	De applicatie ondersteunt IDP initiated login.
Toelichting	Om te voorkomen dat een gebruiker meerdere stappen dient te doorlopen om ingelogd te komen op de SAAS-dienst, ondersteunt de SAAS-applicatie de mogelijkheid om een inlogverzoek te laten initiëren door de IDP. Dit wil zeggen dat, door bijvoorbeeld gebruik te maken een 'slimme url' de SAAS-dienst automatisch de benodigde inlogstappen doorloopt waardoor de eindgebruiker een seamless login experience krijgt.

30	**Indien de applicatie mail moet kunnen versturen dan wordt dat door de opdrachtgever op aanvraag van de opdrachtnemer middels een app registration in Entra-ID ingeregeld**
Toelichting	Mailen vanuit naam van de opdrachtgever geschiet altijd via een app registration in Entra ID. Hiervoor wordt middels een aanvraag door de opdrachtnemer, de inrichting in samenwerking met de opdrachtgever gerealiseerd. Er zal geen whitelisting nodig zijn door opdrachtgever noch aanpassingen in DNS records. (zoals SPF-records)

31	**De applicatie dient (t.a.v. informatiebeveiliging) aantoonbaar te voldoen aan marktconforme certificering of toont dit aan middels het ROSA self assessement dat correspondeert met de BIV-classificatie van de applicatie.**
Toelichting	ROSA self assessment documentatie is te vinden op: Certificeringsschema informatiebeveiliging en privacy ROSA - versie 3.0 - Edustandaard Certificeringsschema ROSA - toetsingskader - versie 3.0

32	**De beveiligingsmaatregelen bij de opdrachtnemer zijn volgens een systematiek ingevoerd**
Toelichting	Een voorbeeld is ISO 27001/27017, combi, ESEA 5402 type II.

33	**De verbinding met de applicatie is te allen tijde versleuteld.**
Toelichting	Als veilige versleuteling wordt de score van 'SSL Labs Server Test' gehanteerd (https://www.ssllabs.com), waarbij een minimaal score A behaald dient te worden. Als tweede wordt een test uitgevoerd bij http://www.internet.nl/ waarvan de resultaten worden geëvalueerd en besproken met de opdrachtnemer indien hier aanleiding voor is.

34	**De opdrachtnemer zal minimaal 1x per dag controleren of de verbinding voldoende veilig is en is in staat om dit, op verzoek van de opdrachtgever, in een rapportage inzichtelijk te maken.**
Toelichting	Om altijd aan te kunnen tonen dat de verbinding veilig is en er adequaat wordt gereageerd op incidenten die ertoe leiden dat de veiligheidsscore (zie eis 29) is verlaagd, is de opdrachtnemer in staat om hiervan een rapportage te overleggen aan de opdrachtgever waarbij minimaal 1x per dag de status wordt vastgelegd.

35	**De opdrachtnemer laat zijn omgeving periodiek, minimaal jaarlijks, onafhankelijk auditen.**
Toelichting	Conform het door de opdrachtnemer aangegeven normenkader zoals vastgelegd in bijlage 2 van de verwerkersovereenkomst en opdrachtnemer deelt de bevindingen van de audit met de opdrachtgever.

36	**De opslag en verwerking van persoonsgegevens vindt uitsluitend plaats in landen binnen de Europese Economische Ruimte (EER) of derde landen met een passend beschermingsniveau.**
Toelichting	Opdrachtnemer geeft in de verwerkersovereenkomst aan waar de opslag en verwerking van persoonsgegevens plaatsvindt. Opdrachtgever accepteert alleen opslag en verwerking van persoonsgegevens binnen de EER of derde landen met een passend beschermingsniveau.

37	**De applicatie is ontworpen met het uitgangsprincipe privacy- en informatiebeveiliging by design.**
Toelichting	De opdrachtnemer toont aan hoe dit wordt toegepast in het ontwikkelproces.

38	**Als de opdrachtnemer test-, cursus- of acceptatieomgevingen aanbiedt, dan is deze gevuld met testdata.**
Toelichting	Er wordt verwacht dat de opdrachtnemer een testdata-strategie heeft waaruit blijkt: - Hoe voorkomen wordt dat productiedata in de testomgeving terecht komt. - Of er gebruik wordt gemaakt van ‘shuffle’ en ‘scramble’ technieken om zo gegevens te anonimiseren.

39	**Certificaten met relatie tot de opdrachtgever, worden door de opdrachtgever aangeleverd en door de opdrachtnemer geïmplementeerd.**
Toelichting	Certificaten worden altijd door de opdrachtgever aangeleverd zodat deze altijd naar de CA (Sectigo) van de opdrachtgever te herleiden is. Oplossingen zoals AWS of Let's Encrypt worden niet geaccepteerd.

9 Performance

40	**De opdrachtnemer is accountable voor (de performance van) de gehele keten van de opdrachtgever tot en met het datacenter van de opdrachtnemer.**
Toelichting	Aangezien opdrachtgever op het Surf netwerk aangesloten is, is de wens dat bij lage performance de opdrachtnemer de regie voert over probleemdefinitie, oplossingsrichtingen en de samenwerking met opdrachtgever organiseert.

41	**De opdrachtnemer is accountable voor (de beschikbaarheid van) de gehele keten van opdrachtgever tot en met het datacenter van de opdrachtnemer.**
Toelichting	Hierbij neemt de opdrachtnemer adequate maatregelen voor bescherming tegen, maar niet beperkt tot, DDoS aanvallen en stroomuitval. Deze worden niet uitgesloten in een overmacht clausule.

42	**De maximale latency is 15ms RTT**
Toelichting	De responstijd van server naar endpoint (van opdrachtnemer naar het eindpunt van Yonder) en terug is maximaal 15 ms.