

Algemeen, Security en Privacy

Algemeen

- 1 De opdrachtnemer voldoet aan het SURF Juridisch Normenkader (Cloud)services, welke te vinden is op: <https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html> en/of beschikt over het ISO 27001 beveiligingscertificaat dat is afgegeven door een officiële instantie, dan wel een gelijkwaardig certificaat.
- 2 De processen rond operationele en tactische ICT-aansturing zijn beschreven en geaccordeerd (beschikbaarheid, calamiteiten, privacy, beveiliging, wijzigingen). Deze passen binnen de geldende kaders/ uitgangspunten en afspraken. Deze beschreven in een Service Level Agreement (SLA) en Dossier van Afspraken en Procedures (DAP), dan wel een Experience Level Agreement (XLA).
- 3 Er is een functioneel ontwerp van de koppelingen, de applicatie en de inrichting daarvan voor Yuvarta voordat deze wordt opgeleverd. Op het functioneel ontwerp is een acceptatieproces van toepassing.
- 4 De inschrijver beschikt over een statuspagina voor wat betreft beschikbaarheid, incidenten en calamiteiten t.a.v. de oplossing.
- 5 Leverancier werkt mee aan het opstellen van een beheerplan voor de ELO. De inrichting en organisatie van het functioneel beheer passen binnen de kaders/ uitgangspunten zoals deze zijn vastgesteld binnen de organisatie. De leverancier adviseert en borcht de invulling van zijn eigen rol in dit beheerplan.

Security

- 6 De opdrachtnemer onderschrijft het nut van security by design en heeft dit volledig doorgevoerd in de oplossing.
- 7 De opdrachtnemer commiteert zich aan security by design en alle voorkomende werkzaamheden om de oplossing en de omgeving waar deze in draait maximaal te beschermen.
- 8 De opdrachtnemer ontwikkelt en beheert de oplossing op basis van of vergelijkbaar aan de CIP-overheid.nl richtlijnen zoals die in de Security Technical IT Checklist staan (STITCH)
- 9 De opdrachtnemer voert minimaal jaarlijks een risicoanalyse uit en deelt de resultaten met de opdrachtgever. Dit houdt minimaal in:
 1. een pentest;
 2. een onafhankelijke audit en /of een risicoanalyse, bijvoorbeeld SOC2 Type II.
- 10 De opdrachtnemer maakt gebruik van Domain Name System Security Extensions (DNSSEC) of vergelijkbaar.
- 11 Het gebruik van de applicatie wordt gelogd. De opdrachtgever kan een verzoek doen tot een rapportage van de logging om in ieder geval te kunnen zien op welk tijdstip iemand bepaalde acties heeft uitgevoerd (de zogenaamde audit trail, waarin alle interacties worden bijgehouden).
- 12 De opdrachtnemer rapporteert proactief over cybersecurity incidenten.
- 13 De opdrachtnemer maakt het mogelijk dat er geen mogelijk dataverlies bij verstoringen optreedt en geeft inzicht gedurende uitvoering hoe dit bewerkstelligd wordt.
- 14 Alle gegevens worden versleuteld getransporteerd.
 - De vertrouwelijkheid, integriteit en onweerlegbaarheid van gegevensleveringen of transacties dient geborgd te worden.
 - Datatransport wordt volgens up-to-date encryptie-standaarden en standaard transportprotocollen versleuteld.
 - Als het transportprotocol geen versleutelingsmogelijkheden biedt, moet de data versleuteld worden.
 - Bij fysiek transport van gevoelige data, zoals USB-sticks, dient de data volgens up-to-date encryptie-standaarden versleuteld te zijn.
 - Certificaatbeheer moet ingericht zijn, certificaten worden geleverd door de opdrachtgever.

Privacy

- 15 De opdrachtnemer onderschrijft het nut van privacy by design en heeft dit volledig doorgevoerd in de oplossing.
- 16 De oplossing en service van de opdrachtnemer voldoet aantoonbaar aan de AVG eisen.
- 17 De opdrachtnemer rapporteert proactief op datalekken.
- 18 De ELO en alle data dienen in de EU (Europese Unie, https://europa.eu/european-union/about-eu/countries_nl) te staan. Indien inschrijver dit in de toekomst wil wijzigen, dient zij hiervoor minimaal 3 maanden voorafgaand aan de gewenste wijziging toestemming te vragen aan opdrachtgever.
- 19 De opdrachtnemer dient mee te werken bij een verzoek in het kader van rechten van betrokkenen (AVG) waaronder het recht om vergeten te worden en het recht op inzage.
- 20 De applicatie en de manier waarop de gegevens opgeslagen worden in de applicatie en hoe er met de gegevens wordt omgegaan, voldoen aantoonbaar aan de Wet Algemene Verordening Gegevensbescherming, zoals vastgelegd in de toepasselijke verwerkersovereenkomst.
- 21 Gegevens die door de opdrachtgever of namens de opdrachtgever aan de inschrijver worden verstrekt middels het gebruik van de ELO worden niet gebruikt voor commerciële doeleinden. Gegevensanalyse ter bevordering van de ELO is wel toegestaan, maar niet voor commerciële doeleinden.

Beschikbaarheid en separate omgeving test en scholing

Beschikbaarheid

- 22 De opdrachtnemer monitort dat er gedurende de volledige looptijd en eventuele verlengingen van het contract wordt voldaan aan het contract en de service level assurance en dat de verwerkingsovereenkomst actueel is. Bij de servicelevel assurance kan bijvoorbeeld worden gedacht aan:
1. Levert een ISAE 34xx audit verklaring of vergelijkbaar
 2. Algemeen risicoanalyse op privacy en security
 3. Leveranciers verbeteringen
 4. Onafhankelijke audit op datacenter etc.
- De opdrachtnemer committeert zich om hier op aanvraag bewijsmaterialen voor aan te leveren en deel te nemen aan de jaarlijkse leveranciersbeoordeling waar deze onderwerpen worden besproken.
- 23 De Recovery Time Objective (RTO) van de applicatie is maximaal 4 uur.
- 24 De Recovery Point Objective (RPO) van de data is maximaal 24 uur.
- 25 De beschikbaarheid van de oplossing moet minimaal 99,9% zijn in het tijdsvenster van 06:00 – 00:00 uur, 7 dagen per week en gerekend op maandbasis.
- 26 De overall beschikbaarheid (24/7) van de oplossing bedraagt tenminste 99,5% (4 uur per maand niet beschikbaar).
- 27 De opdrachtnemer rapporteert proactief over ernstige verstoringen en calamiteiten.
- 28 Het bewaarregime van de opdrachtnemer stelt de opdrachtgever in staat om te allen tijde te voldoen aan de bewaartermijnen.
- 29 **Separate omgevingen t.b.v. test en scholing**
- 30 De oplossing bevat naast de productieomgeving separate omgevingen voor test- en acceptatie doeleinden. De testomgeving kan minimaal gebruikt worden voor het testen van koppelingen en nieuwe releases. In de testomgeving moet het mogelijk zijn om productiegegevens anoniem te maken.
- 31 De acceptatie- en/of testomgeving zijn geschikt voor scholingsdoeleinden waarbij geen toegang is tot persoonlijke data van studenten en docenten.

Data-architectuur, toegang en toegankelijkheid

Data-architectuur

- 32 De oplossing is webgebaseerd en ondersteunt integraties met andere systemen van de opdrachtgever.
- 33 De oplossing ondersteunt minimaal de meest actuele versies van de volgende standaarden:
- SAML
 - OAuth
 - SOAP / REST/Json API
 - LTI (minimaal versie 1.3)
 - SCORM
 - ICaI
 - SCIM
 - OIDC (OpenID Connect)
- 34 Voor de uitwisseling van informatieobjecten uit de bronsystemen van de opdrachtgever kan in alle gevallen gebruik worden gemaakt van de gegevensuitwisselingssleutels uit de bronsystemen.
- 35 Een gedetailleerde beschrijving van het API koppelvlak wordt door de opdrachtgever ter beschikking gesteld, de opdrachtnemer moet daarmee zelf in staat zijn om de integratie met andere systemen van de opdrachtgever te kunnen ontwikkelen.
- 36 Het datamodel wordt beschikbaar gesteld aan de opdrachtnemer.
- 37 De opdrachtnemer wordt minimaal 3 maanden van te voren op de hoogte gesteld van wijzigingen in het datamodel of een van de koppelvlakken.
- 38 Alle gegevens worden versleuteld getransporteerd, met behulp van TLS 1.2 of hoger.
- 39 Data in de toepassing die niet door iedereen ingezien mag worden in de oplossing kan op basis van rollen worden afgeschermd; het is mogelijk om met autorisaties data toegankelijk of ontoegankelijk te maken voor specifieke rollen.
- 40 De opdrachtnemer geeft compleet inzicht in de informatiestroom en welke partijen daarbij betrokken zijn. Deze partijen en het aandeel in de verwerking moeten zijn opgenomen in de verwerkersovereenkomst.

Toegang

- 41 De oplossing ondersteunt meerdere authenticatiebronnen tegelijkertijd.
- 42 De oplossing kan gebruikmaken van Surf Conext Single Sign On.
- 43 De oplossing kan gebruikmaken van Kennisnet Single Sign On.
- 44 De oplossing kan gebruikmaken van de MFA oplossing van Microsoft op basis van conditional access policies
- 45 Autorisatie is (mede) op basis van rollen.

Toegankelijkheid

- 46 De gebruikersinterface is in het Nederlands en het Engels beschikbaar.
- 47 De ELO moet toegankelijk zijn vanaf zowel de thuis-, school- als /werkomgeving via verschillende devices (tenminste desktop, laptop, smartphone, tablet).

Dataportabiliteit en exitstrategie

Dataportabiliteit en Exit strategie

- 48 Bij beëindiging van deze Overeenkomst om welke reden dan ook, dan wel op eerste verzoek van opdrachtgever gedurende de looptijd van de Overeenkomst, zal opdrachtnemer –zonder kosten- ervoor zorgdragen dat naar keuze van opdrachtgever
- (i) alle hem in het kader van de Clouddienst ter beschikking gestelde gegevens worden vernietigd,
 - (ii) alle hem in het kader van de Clouddienst ter beschikking gestelde gegevens aan een opvolgend dienstverlener ter beschikking worden gesteld, dan wel
 - (iii) opdrachtgever en/of gebruikers in de gelegenheid worden gesteld om hun gegevens aan de Clouddienst te onttrekken.
- Opdrachtgever kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling dan wel vernietiging.
- 49 De opdrachtnemer zal te allen tijde de in het vorige lid beschreven dataportabiliteit van de gegevens waarborgen zodanig dat er geen sprake is van verlies aan consistentie van de gegevens.
- 50 De opdrachtgever kan vrij (op elk moment, zonder extra kosten of zonder extra handelingen door de opdrachtnemer) beschikken over de eigen opdrachtgever gegevens voor het exporteren daarvan.
- 51 Er is een up-to-date Escrow-overeenkomst die de continuïteit t.a.v. de software waarborgt, minimaal volgens Escrow voor SaaS: <https://www.escrowalliance.com/nl/escrow-regelingen/saas-escrow-regeling/>

Infrastructuur

Infrastructuur

- 52 De opdrachtnemer garandeert dat de ingebruikname van de clouddienst géén aanpassingen in de opdrachtgever IT infrastructuur vereist.
- 53 Op werkpleksystemen van gebruikers wordt voor een normale werking geen aparte cliëntsoftware geïnstalleerd. Uitzondering hierop kan zijn een app voor een tablet of andere mobiele apparaten.
- 54 Minimaal de volgende webbrowsers met de op elk moment meest recente versies worden ondersteund:
- Edge Chromium
 - FireFox
 - Safari
 - Chrome

Bijeenkomsten en escalatieprocedure

Bijeenkomsten en escalatieprocedure

- 55 De opdrachtnemer stemt tenminste in de volgende frequentie, zowel tijdens als na de implementatie, af met de opdrachtgever:
- Operationeel overleg (wekelijks)
 - Tactisch overleg (per kwartaal)
 - Strategisch overleg (jaarlijks)
- Afhankelijk van het type overleg (operationeel, tactisch, strategisch) waarborgt de opdrachtnemer dat de deelnemers aan de kant van de opdrachtnemer over het juiste profiel beschikken om een goede gesprekspartner te zijn voor dat type overleg.
- 56 De opdrachtnemer stelt met de opdrachtgever een escalatieprocedure vast, welke wordt vastgelegd in de SLA.

Ondersteuning en scholing

Ondersteuning en scholing

- 57 De leverancier levert voor de verschillende gebruikersgroepen de benodigde gebruikersdocumentatie aan. Yuverta kan delen van deze documentatie hergebruiken in andere gebruikersdocumentatie en voor andere doelen dan de directe ondersteuning van het ELO-gebruik. Gebruikersdocumentatie kan in verschillende verschijningsvormen kennen zoals, maar niet uitsluitend, fysieke en digitale documenten, video, audio, html, etc.
- 58 De ondersteuningsorganisatie, bestaande uit de helpdesk en consultancy-medewerkers, is in Nederland gevestigd en voert de Nederlandse taal.