Bijlage 4a Programma van Eisen m.b.t. Clouddiensten, behorende bij aanbesteding "Levering en onderhoud van rittenregistratie" met registratienummer 21.0083180

Uitgangspunten	ja/nee
A. De toepasselijke algemene inkoopvoorwaarden maken deel uit van de overeenkomst;	
B. Basisprincipes zoals functiescheiding, least privilege, need to know, en meerdere "layers of defense" (defense in depth) zijn standaard een uitgangspunt voor de overeen te komen maatregelen met de leverancier;	
C. Er wordt overeengekomen tot welke informatie-assets de leverancier toegang heeft en welke toegangsvormen zijn toegestaan;	
D. Van de leverancier wordt verwacht dat zij adequate beheersing uitoefent ten aanzien van de informatiebeveiliging bij haar leverancierskеten die betrokken is bij het leveren van een dienst of product aan HHNK;	
E. HHNK heeft het recht om de leverancier en de betrokken leverancierskеten te auditen ten aanzien van de informatiebeveiliging;	
F. De inrichting van de incidentmanagement, calamiteitenprocedures en flexibiliteitsafspraken met inbegrip van de wederzijdse verantwoordelijkheden zijn gebaseerd op een risico assessment;	
G. De leverancier zorgt ervoor dat haar processen, producten en diensten voldoen aan expliciet overeengekomen, toepasselijke (technische) normen;	
H. De leverancier moet voldoen aan de door HHNK aangeleverde aanvullende beveiligingseisen.	
1. Algemeen	
A. Het informatiesysteem wordt binnen een SaaS, PaaS of IaaS omgeving uitgevoerd;	
B. De leverancier stelt een testomgeving beschikbaar voor de HHNK;	
C. De leverancier zelf, noch haar eigenaar(s) of aandeelhouders, noch haar nationaliteit of vestigingslocatie vormen een risico voor HHNK, waarin inbegrepen risico's ten aanzien van ongewenste (buitenlandse) beïnvloeding;	
D. De leverancier zorgt ervoor dat de datacenters waar de omgevingen draaien minimaal ISO 9001, 14001 en 27001 gecertificeerd zijn.	
2. Vermijd gebruik	

A. Onvoldoende verantwoorde omgang met gevoelige gegevens van bedrijven en burgers, waar de volgende situaties zijn inbegrepen:	
1. Er is sprake van persoonsgegevens en er kan niet voldaan worden aan de AVG;	
2. Er is sprake van medewerkersgegevens en de persoonlijke veiligheid van de medewerker is in het geding en ondanks mitigerende maatregelen blijft er sprake van een te hoog restrisico.	
B. Als er sprake is van cruciale belangen, zoals informatie met een vertrouwelijkheidsclassificatie **hoog** of een Integriteitsclassificatie **hoog**;	
C. Er ontstaan risico's voor het primair proces op **BBN2** niveau of hoger, en ondanks mitigerende maatregelen blijft er sprake van een te hoog restrisico.	
3. Naleving	

A. Een geheimhoudingsverklaring;	
B. Medewerkers van de leverancier doorgaan bij indiensttreding een screeningsproces;	
C. Een verwerkersovereenkomst als de verwerking van persoonsgegevens tot de mogelijkheden behoort, waarbij HHNK de verwerkingsverantwoordelijke is, en de leverancier de hoofdverwerker is die handelt conform expliciete instructies van uitsluitend HHNK;	
D. De voor de leverancier eigen relevante wettelijke eisen (zoals AVG eisen en encryptie toepassing) om persoonsgegevens te kunnen beschermen;	
E. De naleving van alle voor HHNK van toepassing zijnde vereisten die voortvloeien uit de Nederlandse- en EU wet- en regelgeving, zoals de AVG, de Uitvoeringswet AVG, de wet meldplicht datalekken, en de door de Autoriteit Persoonsgegevens gestelde aanvullende regelingen met bijzondere aandacht voor het niet toepassen van geografisch verspreide opslag buiten de EU en verwerkingen buiten de EU;	
F. Op welke wijze het informatiesysteem voldoet aan de landelijk gehanteerde standaard 'ICT-beveiligingsrichtlijn voor webapplicaties' van de NCSC;	
G. De leverancier voorziet HHNK van zekerheid (evidence based compliance rapportage) over (het voldoen aan) de van toepassing zijnde wettelijke eisen en contractuele vereisten;	
H. De specifieke maatregelen die getroffen zijn, en de verantwoordelijkheden die zijn benoemd om aan alle wettelijke- en contractuele eisen te voldoen.	
4. Beveiligingsbeleid	
A. De leverancier heeft een beveiligingsbeleid dat organisatorische uitgangspunten bevat;	
B. De leverancier heeft een beveiligingsbeleid dat technische uitgangspunten bevat;	
C. De leverancier heeft een beveiligingsbeleid dat specifieke uitgangspunten bevat die van toepassing zijn op het aanbieden van Clouddiensten.	
5. Beveiligingsstrategie	

A. De passende technische en organisatorische maatregelen, conform de maatregelen genoemd in de BIO genomen zodat gegevens niet verloren gaan, worden gemanipuleerd of in onbevoegde handen vallen;	
B. Veilige toegang tot het informatiesysteem middels authenticatie- en autorisatieservices. Waarbij privacyaspecten onderdeel uitmaken van de autorisatie in het systeem;	
C. Het afstemmen van autorisaties op de rol van de diverse actoren en de noodzakelijkheid van deze rol om te beschikken over c.q. het bewerken van persoonsgegevens;	
D. De centrale logging van het informatiesysteem en het afschermen daarvan;	
E. Het voorzien van gegevens van een bewaartermijn om deze niet langer te bewaren dan noodzakelijk is.	

6. Transparantie	
A. De leverancier voorziet HHNK van een systeembeschrijving waarin de Clouddiensten inzichtelijk en transparant worden gespecificeerd, waarin onder meer de relatie zichtbaar is:	
1. tussen de afgenomen dienst en de infrastructuur;	
2. tussen de opslag- en verwerkingslocaties;	
3. tussen de uitbestede diensten / onderaannemers;	
4. van de onderzoeksmogelijkheden	
7. Exit strategie	
A. HHNK kan eenzijdig een exit in gang zetten als:	
1. De afgesproken dienstverlening of performance niet wordt geleverd;	
2. De SLA of geleverde dienst eenzijdig door de leverancier wordt gewijzigd;	
3. De prijs wordt verhoogd, ook al gaat dit gepaard met een uitbreiding of aanpassing van de dienstportfolio of de prestatie niveaus;	
4. Er onvoldoende compensatie voor storingen plaatsvindt;	
5. Gebrekkige ondersteuning plaatsvindt;	
6. De leverancier een nieuwe eigenaar krijgt;	
7. De leverancier een andere strategie kiest;	
8. Er sprake is van een end-of-life situatie van de Clouddiensten;	
9. Als features achterwege blijven, waarin begrepen het niet voldoen aan actuele wet- en regelgeving, de-facto industriestandaarden, en actuele besturingssystemen;	
B. Bij een exit zijn de volgende afspraken van toepassing:	
1. De exit bepaling geldt zowel bij het einde van de overeenkomst als om valide redenen aangedragen door HHNK;	
2. De overeenkomst (evenals deelovereenkomsten zoals een eventuele verwerkersovereenkomst of een DAP) duurt voort totdat de exit regeling helemaal is uitgevoerd;	
3. De opzegtermijn geeft voldoende tijd om te kunnen migreren;	
4. De leverancier zal tegen een van tevoren overeengekomen tarief meewerken aan een migratie naar een nieuw systeem, of de volledige gegevens set van de opdrachtgever in een geordende staat, in een formaat dat voldoet aan internationale standaarden en voorzien van een adequate beschrijving opleveren aan HHNK;	
5. Data en configuratiegegevens (indien relevant) mogen pas na succesvolle migratie naar een nieuw systeem verwijderd worden;	
6. Bij verwijdering worden alle gegevens vernietigd, inclusief de backup gegevens en metadata;	
7. Door een onafhankelijke partij kan worden gecontroleerd en vastgesteld dat alle data is gemigreerd;	
8. De exit regeling wordt aangepast/anders ingevuld als de software die gebruikt wordt voor de Clouddienst is gewijzigd.	
8. Gegevens	
A. De gegarandeerde opslagduur is expliciet overeengekomen met de leverancier en voldoet aan de archiefwet of door HHNK bepaalde bewaartermijn;	
B. Gegevens zijn onafhankelijk van de door de leverancier toegepaste technologie raadpleegbaar door HHNK gedurende de gehele bewaartermijn;	
C. Alle gegevens zijn en blijven te allen tijde eigendom van HHNK, zijn ten alle tijden toegankelijk en mogen door de leverancier niet voor andere doeleinden worden gebruikt.	
9. De Clouddienst omgeving	
A. De leverancier is verantwoordelijk voor een beveiligde en bedrijfszekere systeemomgeving;	
B. De leverancier garandeert dat gegevens in het informatiesysteem worden veilig gesteld middels back-up;	
C. De leverancier garandeert dat ongeautoriseerde personen geen toegang hebben tot gegevens of gegevensdragers (zoals harde schijven en back-upmedia) die tussentijds of na beëindiging van de overeenkomst worden verwijderd c.q. worden vervangen;	
D. Op de gegevens van de HHNK wordt encryptie toegepast;	
E. Om de interoperabiliteit van Cloud Services te garanderen zijn gegevens beschikbaar conform erkende industriestandaarden en gedocumenteerde invoer- en uitvoerinterfaces.	
F. Er is een totaaloverzicht beschikbaar van autorisaties van zowel leverancier als HHNK;	
G. De leverancier zal ongeautoriseerde toegang tot de systeemomgeving signaleren, en alle noodzakelijke maatregelen nemen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. De (poging tot) ongeautoriseerde toegang alsmede alle getroffen maatregelen zullen aan de Opdrachtgever worden gerapporteerd;	
H. Situaties waarin meer dan normale kwetsbaarheden, risico's of beveiligingsincidenten aanwezig zijn (zoals een datalek) worden onmiddellijk gemeld aan en besproken met de HHNK hoe deze op te lossen en te voorkomen in de toekomst;	
I. Twee-factor authenticatie wordt ondersteund;	
J. Gebruikers op afstand moeten beschikken over een combinatie van authenticatiemiddelen voor toegang tot het informatiesysteem;	
K. In overleg kan voor gebruikers die vanuit een benoemd LAN inloggen single sign on of username/wachtwoord worden toegepast voor toegang tot het informatiesysteem (verplicht bij een vertrouwelijkheidsclassificatie **hoog**);	
L. Bij datacommunicatie voor gegevensuitwisseling wordt gebruik gemaakt van tweezijdige authenticatie middels certificaten met een sleutellengte van 2048 bits;	
M. IT-voorzieningen en apparatuur bij leverancier zijn fysiek beschermd tegen toegang door Onbevoegden en tegen schade – zowel door interne als externe oorzaken - en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico's;	
N. Systeemsoftware die bij leverancier in gebruik is, wordt up-to-date gehouden;	

O. Systeemsoftware die bij de leverancier in gebruik is, wordt tijdig voorzien van de laatste security patches;	
P. Wijzingen in het informatiesysteem of daaraan gerelateerde informatiesystemen die van invloed zijn op de werking worden uitgevoerd volgens een vastgestelde wijzigingsprocedure met minimaal aandacht voor:	
1. het administreren van significante wijzigingen;	
2. impactanalyse van mogelijke gevolgen van de wijzigingen;	
3. goedkeuringsprocedure voor wijzigingen;	
4. Tijdige communicatie met de HHNK.	
Q. Pieken in gebruik worden adequaat opgevangen door extra capaciteit op alle relevante onderdelen beschikbaar te stellen;	
R. Het informatiesysteem is schaalbaar. Noodzakelijke uitbreidingen om het informatiesysteem te laten functioneren (bijvoorbeeld beschikbaarheid dataopslag, beschikbaarheid CPU, etc..) worden door de leverancier tijdig gesignaleerd, aangepast en gemeld bij HHNK;	
S. De leverancier zorgt ervoor dat HHNK geen last heeft van onwenselijk gedrag van andere klanten en hard- en software componenten in de omgeving van de Cloud oplossing;	
T. Waar virtualisatie wordt toegepast zorgt de leverancier voor afdoende isolatie van componenten van HHNK en andere klanten;	
U. De leverancier zorgt er voor dat netwerkverkeer tussen verschillende omgevingen niet kan worden onderschept door andere klanten die actief zijn binnen de systeemomgeving van de leverancier.	
10. Beschikbaarheid Clouddienst omgeving	
A. De leverancier voorkomt dat gebruik van gedeelde componenten door andere klanten in de infrastructuur de performance bedreigen;	
B. De leverancier zorgt dat inbeslagname van kritieke componenten, als gevolg van een dwangbevel gericht op een andere klant, voor HHNK geen nadelige gevolgen heeft;	
C. De leverancier waarborgt dat de ondersteuning van, voor HHNK belangrijke technologie, blijvend wordt ondersteund;	
D. De leverancier beschrijft hoe beschikbaarheidsrisico's worden beperkt via technische maatregelen; bijvoorbeeld via redundantie in componenten in de netwerk-, server- en opslaglagen;	
E. De leverancier monitort het informatiesysteem om beschikbaarheids-, security- en schaalbaarheidsrisico's uit te sluiten;	
F. Het informatiesysteem is tijdens openingstijden 98% op maandbasis beschikbaar voor alle partijen (ook in piekperiodes). Dit is exclusief geplande en onvermijdbare downtime voor een nieuwe release. Geplande downtime wordt in overleg met HHNK vastgesteld. Bij een storing waardoor het informatiesysteem niet beschikbaar is (ook niet met omwegen) geldt een oplostijd van maximaal 16 werkuren (twee dagen van 8 uur);	
G. De leverancier beschrijft hoe wordt omgegaan met crisissituaties waarbij technische verstoringen optreden; bijvoorbeeld welke uitwijkprocedures beschikbaar zijn om continuïteit voor HHNK te borgen;	
H. De leverancier laat door een externe partij periodieke audits uitvoeren op de hierboven genoemde onderdelen en stelt deze beschikbaar aan HHNK. De methodiek van audit sluit aan bij de op dat moment geldende wettelijke standaarden.	
11. Beheersing van de dienstverlening en de informatiebeveiliging	
A. De leverancier heeft voor de Clouddiensten een Service Management beleid geformuleerd met daarin richtlijnen voor de beheersingsprocessen, controleactiviteiten en rapportages:	
1. De leverancier beschikt voor de Clouddiensten over richtlijnen voor de inrichting van de Service Management organisatie.	
2. De leverancier beschikt ten aanzien van Clouddiensten over richtlijnen voor het:	
- uitvoeren van controle-activiteiten, waaronder penetratietests en kwetsbaarheid testen;	
- evalueren en rapporteren over de performance en leveringsprestaties;	
- evalueren escalatieproces voor de geleverde diensten;	
B. De leverancier behoort jaarlijks de naleving van de Cloud beveiligingsovereenkomsten op compliancy te beoordelen, jaarlijks een assurance verklaring afgegeven door een onafhankelijke derde partij aan de leverancier uit te brengen en ervoor te zorgen voor onderlinge aansluiting van de resultaten uit deze twee exercities.	