Algemene Voorwaarden Onesurance

1. Inleiding

Wij informeren u graag over wat u van ons mag verwachten bij het gebruik van onze AI-as-a-Service. Deze voorwaarden zijn opgesteld in begrijpelijke taal om transparantie te waarborgen. Indien er onduidelijkheden zijn, staan wij open voor uw vragen..

2. Geldigheid Voorwaarden

Deze Voorwaarden maken deel uit van onze overeenkomst en gelden gedurende de looptijd, inclusief eventuele verlengingen.

3. Wijziging Voorwaarden

De meest recente versie van de Voorwaarden is altijd van toepassing. Wijzigingen worden tijdig gecommuniceerd en klanten hebben de mogelijkheid deze niet te accepteren, met een opzegtermijn van twee maanden onder de oude voorwaarden.

4. Looptijd AI-as-a-Service

De overeenkomst geldt voor onbepaalde tijd, tenzij anders overeengekomen. De opzegtermijn voor klanten is twee maanden voor de nieuwe jaarperiode, terwijl wij een opzegtermijn van zes maanden hanteren voor evenredigheid. Met onze AI-as-a-Service krijgt u een licentie voor het gebruik van onze software en recht op aanvullende dienstverlening. Voor deze licentie en dienstverlening brengen wij het overeengekomen tarief in rekening en ontvangt u elk maand een factuur.

5. Licentie en aanvullende dienstverlening

In de AI-as-a-Service zijn de productonderdelen opgenomen die u afneemt op basis van de tariefbasis (aantallen polissen). Aanvullend betaalt u een vast bedrag per maand voor Hosting & Rekenkracht. De onderdelen vindt u terug op uw factuur. U mag de licentie alleen gebruiken voor uw eigen organisatie of diens dochterondernemingen. Naast de licentie voor gebruik van onze software biedt de AI-as-a-Service ook recht op de volgende aanvullende dienstverlening:

- ✓ het oplossen van storingen en het geven van support tijdens de eerste drie maanden, voor zover dat het aantal van 100 supporturen niet overschrijft;
- ✓ continue monitoring van de software en het doorvoeren van nieuwe releases;
- ✓ minimaal eenmaal per jaar een periodieke rapportage inclusief bespreking met het MT van Opdrachtgever;
- ✓ consultancy voor zover specifiek is vermeld.

Indien u behoefte heeft aan extra dienstverlening, hier niet genoemd, zijn wij hiermee graag van dienst. In dat geval zullen wij u aangeven welke kosten wij daarvoor in rekening zullen brengen, indien van toepassing.

6. Leveringstermijnen

Wij vinden het belangrijk om ons aan onze afspraken te houden. Maar soms zijn er onvoorziene omstandigheden of zijn we afhankelijk van derden. Daarom zijn alle door ons opgegeven termijnen bedoeld als indicatief; de enkele overschrijding van een opgegeven termijn brengt ons niet in verzuim. In alle gevallen waarin overschrijding van een termijn dreigt of een termijn niet wordt gehaald, zullen wij zo spoedig mogelijk met elkaar in overleg treden en een redelijke termijn te bepalen om alle verplichtingen alsnog goed na te komen.

7. Onderhoud en storing

Wij kunnen de uitvoering van de AI-as-a-Service geheel of gedeeltelijk buiten gebruik stellen voor onderhoud. Wij zullen onze dienst niet langer buiten gebruik stellen dan noodzakelijk is en zullen dit, indien mogelijk, buiten kantooruren laten plaatsvinden. Storingen zullen we uiteraard zo snel mogelijk oplossen. Voor reactietijden verwijzen we naar de Service Levels in onze Servicevoorwaarden.

8.Garantiebeperking

De AI-voorspellingen zijn gebaseerd op statistische modellen en worden geleverd op basis van best effort. Onesurance aanvaardt geen aansprakelijkheid voor het niet uitkomen van voorspellingen of voor besluiten die Opdrachtgever neemt op basis van deze voorspellingen.

9. Tariefbasis

Voor het tarief van de licentie werken we op basis van het aantal polissen in uw portefeuille, waarvoor we een voorspelling doen. Per productonderdeel geldt een vast bedrag per polis per jaar. De tariefbasis is het aantal polissen afgerond op tienduizend naar beneden. Eenmaal per jaar wordt de tariefbasis opnieuw bepaald en verhogen of verlagen we het tarief op basis van de aantallen. We indexeren jaarlijks de prijzen en houden hierbij rekening met het Consumentenprijsindex-cijfer (CPI) van het afgelopen jaar, de jaarmutatie van juli van het huidige jaar. De indexering gaat in vanaf de eerste factuur in het volgende kalenderjaar. Wij zullen u telkens informeren over de indexering.

10.Facturatie

Tarieven worden jaarlijks geïndexeerd conform het CPI-cijfer van het CBS (jaar-op-jaar juli). Bij uitbreiding van het aantal polissen kan Onesurance het tarief proportioneel aanpassen. Wij factureren de licentie per maand vooraf. U krijgt al onze facturen per e-mail in pdf-bestand. De betalingstermijn is dertig dagen.

11. Aanpassen overeenkomst

Het toevoegen van productonderdelen kan op elk moment. Het afvoeren van productonderdelen kan pas één jaar na volledige facturatie of na afloop van de initiële periode als deze is overeengekomen. Houd er rekening mee dat u een mutatie en/of een beëindigingsverzoek één maand voor de nieuwe facturatieperiode door moet voeren en dat u niet binnen hetzelfde kwartaal kunt verhogen en verlagen.

12.Beëindiging overeenkomst

U kunt de licentie steeds één jaar na volledige facturatie opzeggen. Houd er rekening mee dat u dit twee maanden voor het verstrijken van de nieuwe jaarperiode schriftelijk of per email aan ons meldt. U kunt de licentie tussentijds opzeggen binnen tien werkdagen na afloop van de eerste initiële periode van drie maanden. Na beëindiging van de overeenkomst heeft u geen toegang meer tot de software en bijbehorende data. Uw data zal binnen veertien dagen verwijderd worden. Onze opzegtermijn is twaalf maanden. Wij kunnen de overeenkomst per direct beëindigen als u afspraken niet nakomt en wij u daarvoor in gebreke hebben gesteld, facturen structureel te laat betaalt of een factuur waarover geen discussie bestaat na 60 dagen nog niet hebt betaald. Dit recht hebben wij ook als u surseance van betaling of een faillissement hebt aangevraagd. Na beëindiging van de overeenkomst blijft data gedurende 30 dagen beschikbaar voor export door Opdrachtgever, tenzij schriftelijk anders overeengekomen.

13. Aansprakelijkheid

Wij doen er alles aan om te zorgen dat onze software voldoet aan de specificaties die we opgeven. Als er toch fouten zijn, herstellen we die zo snel mogelijk. Wij willen dat onze software optimaal werkt en ook onze dienstverlening moet goed zijn. Toch kunnen er dingen verkeerd gaan. Als u daardoor schade hebt, zoeken we samen naar een passende oplossing. Als u een klacht of claim hebt, is het zaak dat u die zo snel mogelijk bij ons meldt. Wij kunnen dan direct aan de slag om een oplossing te vinden. Bovendien moeten wij een claim ook melden bij onze verzekeraar. Wat er ook misgaat, wij willen altijd in goed overleg de juiste oplossing vinden. Onze totale aansprakelijkheid wegens een toerekenbare tekortkoming in de nakoming van de overeenkomst of op welke rechtsgrond dan ook is beperkt tot vergoeding van directe schade tot maximaal het bedrag van de voor die overeenkomst bedongen prijs (excl. BTW). Indien de overeenkomst hoofdzakelijk een duurovereenkomst is met een looptijd van meer dan één jaar, wordt de voor die overeenkomst bedongen prijs gesteld op het totaal van de vergoedingen (excl. BTW) bedongen voor één jaar. In beide situaties is onze maximale cumulatieve aansprakelijkheid beperkt tot EUR 50.000,-. Wij kunnen uitsluitend aansprakelijk worden gehouden tot vergoeding van directe schade en niet voor enige vorm van gevolgschade. Onder gevolgschade worden in ieder geval begrepen gederfde omzet, gederfde winst, verlies van gegevens en gemiste kansen. Wij zijn beide niet aansprakelijk ten opzichte van elkaar bij overmacht in de zin van de wet. Dit geldt ook bij overmacht van toeleveranciers, storingen in het elektriciteitsnet en storingen die dataverkeer belemmeren als de oorzaak daarvan niet is te wijten aan partijen zelf. Bij opzet of bewuste roekeloosheid door ons bedrijf en/of onze leidinggevende medewerkers kunnen wij geen beroep doen op de aansprakelijkheidsbeperkingen.

14. Intellectueel eigendomsrecht

Het intellectuele eigendomsrecht van de software ligt en blijft bij ons. Als een derde anders beweert, zullen wij u vrijwaren. Voorwaarde is wel dat u ons hierover zo spoedig mogelijk informeert, meewerkt aan het onderzoek en ons de zaak laat afhandelen. Als de rechter vaststelt dat het intellectuele eigendom inderdaad bij een derde ligt, zorgen wij dat u de software kunt blijven gebruiken of we bieden gelijkwaardige software aan. U krijgt gedurende de looptijd van de overeenkomst een niet-exclusief, niet-overdraagbaar, niet-verpandbaar en niet-sublicentieerbaar gebruiksrecht op onze software waaronder begrepen gebruik van onze algoritmes. Het is niet toegestaan om zonder voorafgaande schriftelijke toestemming de software en/of algoritmes en/of onze documenten en materialen geheel of gedeeltelijk te verveelvoudigen, openbaar te maken, te reverse-engineeren, te decompileren of aan derden ter hand te stellen en/of ter inzage te geven. De door

Opdrachtgever aangeleverde data blijft eigendom van Opdrachtgever. Opdrachtgever verleent Onesurance een gebruiksrecht voor de looptijd van de overeenkomst om deze data te verwerken t.b.v. dienstverlening, kwaliteitsverbetering en benchmarking, mits geanonimiseerd.

15. Privacy & geheimhouding

Wij zullen alle toepasselijke vereisten uit de Algemene Verordening Gegevensbescherming naleven. Wij garanderen naar elkaar dat alle informatie, waarvan wij redelijkerwijs moeten begrijpen dat deze informatie vertrouwelijk of concurrentiegevoelig is, die wij voor en na het aangaan van de overeenkomst van elkaar ontvangen vertrouwelijk blijft. Wij zullen alle redelijke maatregelen nemen om deze informatie te beschermen. Wij willen er graag in reclame-uitingen of bij marketingactiviteiten melding van kunnen maken dat u één van onze gewaardeerde cliënten bent. Wij zullen daarbij zorgvuldig alle informatie over de resultaten en/of over de bij uw uitgevoerde werkzaamheden die naar u terug kunnen herleiden uit de te gebruiken of te publiceren informatie verwijderen.

16. Juridische zaken

Alle geschillen die voortvloeien uit of verband houden met onze overeenkomst zullen uitsluitend worden onderworpen aan het oordeel van de bevoegde rechter te Breda. Op onze overeenkomst, alsmede op alle geschillen die verband houden met of voortvloeien uit onze overeenkomst, is uitsluitend het Nederlands recht van toepassing. Het Verdrag der Verenigde Naties inzake internationale koopovereenkomsten betreffende roerende zaken (Weens Koopverdrag) is niet van toepassing. Kennisgevingen die wij op grond van deze overeenkomst aan elkaar doen, vinden schriftelijk plaats. Onder schriftelijk wordt verstaan per post en/of per e-mail, indien gericht aan de e-mailadressen van de ondertekenaars van de overeenkomst. Eventuele mondelinge toezeggingen en afspraken hebben geen werking, tenzij deze schriftelijk door beide partijen zijn bevestigd.

17. Partnerstrategie en Training

Implementatiepartners kunnen gecertificeerd worden via een trainingsprogramma. Betaalde onboarding- en trainingsmodules beschikbaar om efficiëntie en adoptie te verhogen.

Contactgegevens Onesurance B.V.

- Bezoekadres: : Rithmeesterpark 50 A1, 4838 AZ Breda | Basisweg 32, 1043 AP Amsterdam
- Email : info@onesurance.nl
- Website : www.onesurance.ai
- K.v.k. : 87521997
- IBAN : NL25 INGB 0398 4072 82
- BTW : NL 8643.18.315.B01

Servicevoorwaarden Onesurance

1. Inleiding

Partijen wensen elkaars verwachtingen en verplichtingen m.b.t. de uitvoering van de dienstverlening, zoals beschreven in de Overeenkomst, kwalitatief te managen. Bij iedere samenwerking hangt het succes af van een juiste en tijdige onderlinge samenwerking. Het is o.a. van belang dat Partijen over en weer duidelijk communiceren, waarbij (belangrijke) informatie tijdig wordt gedeeld.

In deze SLA zijn de afspraken voor de uitvoering van de Dienst vastgelegd.
Overeenkomst Partijen hebben een Overeenkomst tot gebruik van de AI-as-a-Service van Onesurance (hierna: “Overeenkomst”). Deze Service Level Agreement (hierna te noemen de “SLA”) is een onderdeel van deze Overeenkomst.
Toepasselijkheid Deze SLA is van toepassing op de productieomgeving van de AI-as-a-Serviceverlening van Onesurance en bijbehorende portalen en koppelingen. Daarnaast is er, indien overeengekomen, een acceptatieomgeving beschikbaar, voorwaarden hiervoor worden los vermeld.
Doel SLA In de SLA zijn afspraken vastgelegd over de kwaliteitsparameters van de dienstverlening met als doel de kwaliteit en uitvoering van de dienstverlening van zowel het product als de ondersteuning te monitoren en te rapporteren. De SLA heeft betrekking op de Beschikbaarheid van de AI-as-a-Service, de Back-up en doorlopende Beschikbaarheid van gegevens, alsmede de continuïteit van de dienstverlening vanuit Onesurance. Hierbij valt te denken aan de Diensten van Support.
Wijzigingen op bestaande SLA Deze SLA is een levend document dat regelmatig moet worden herzien en bijgewerkt om te blijven voldoen aan de behoeften van beide Partijen. Alle verbeteringen worden eenzijdig doorgevoerd. Indien een aanpassing negatief kan uitpakken voor de Opdrachtgever zal Onesurance dit in overleg doen en pas na akkoord van Opdrachtgever doorvoeren.
Definities Begrippen die met een hoofdletter zijn aangeduid, hebben de volgende betekenis dan wel de betekenis zoals elders in dit document is bepaald:
Acceptatie: de definitieve en schriftelijke goedkeuring door Opdrachtgever van (onderdelen van) de Dienst(en).
Afhandeltijd: de door Leverancier gemeten en geregistreerde tijd (inclusief Responsetijd) tussen:

- Het tijdstip van melden van het Incident bij Leverancier en de melding van Leverancier aan Opdrachtgever dat het Incident verholpen is;
- Het tijdstip waarop dit door Leverancier aantoonbaar is gemeld;
- Het tijdstip dat de Dienst weer beschikbaar is.

Back-up: een kopie van bestanden, gegevens die op een gegevensdrager staan om deze informatie te kunnen herstellen in het geval van een systeemcrash, dataverlies of andere calamiteiten.
Beschikbaarheid: tijdvak uitgedrukt in een percentage van de totale tijd gemeten over een volledige kalendermaand, waarin een Dienst onder de juiste condities beschikbaar is.
Call: een bericht (telefonisch/per e-mail) van een persoon uit de organisatie van Opdrachtgever of een notificatie van het monitoringsysteem van Onesurance.
Datalek: een inbreuk op de vertrouwelijkheid en/of op de integriteit en/of op de Beschikbaarheid van persoonsgegevens waarbij ongeautoriseerde personen onbedoeld of ongeoorloofd toegang hebben gekregen tot (cliënt-)persoonsgegevens Dit kan het gevolg zijn van verschillende oorzaken, zoals een cyberaanval, menselijke fouten, technische storingen of technische fouten. Een Datalek kan resulteren in de ongeoorloofde toegang tot, de openbaarmaking van, de Wijziging van, of het verlies van persoonsgegevens.

Dienst(en): alle door Leverancier krachtens deze Overeenkomst ten behoeve van Opdrachtgever te verrichten werkzaamheden, inclusief alle Diensten, functies en verantwoordelijkheden die niet specifiek in deze Overeenkomst zijn beschreven, maar die nodig zijn voor de juiste en/of wettige uitvoering en levering van de beschreven Diensten, functies en verantwoordelijkheden.
Downtime: de periode waarin de Dienst niet bereikbaar is of in het geheel niet reageert.
Feestdagen: door de overheid vastgestelde nationale Feestdagen en de dagen waarop Leverancier aangekondigd heeft gesloten te zijn. Deze dagen worden niet als Werkdag gerekend.
Gebruikers: de personen die in dienst zijn bij of werkzaam zijn voor Opdrachtgever en/of gebruik maken van de Acceptatie Assistent omdat ze klant/cliënt zijn van Opdrachtgever.
Geplande Niet-Beschikbaarheid: de periode(s) waarbij Acceptatie Assistent niet beschikbaar is als gevolg van geplande en vooraf aangekondigde (onderhouds-)werkzaamheden.
Implementatie: het geheel van handelingen en maatregelen nodig om alle onderdelen van de Diensten en geleverde programmatuur, afzonderlijk en in onderlinge samenhang, in gebruik te kunnen nemen in de organisatie van Opdrachtgever, zodanig dat alle Gebruikers van Opdrachtgever ermee kunnen werken overeenkomstig het overeengekomen gebruik. Tot de Implementatie behoort, indien overeengekomen, tevens de conversie, het realiseren van de voor het overeengekomen gebruik noodzakelijke koppelingen en het uitvoeren van de acceptatieprocedure.
Incident: een onderbreking, afwijking, verstoring, verminderde Beschikbaarheid of verminderde snelheid van een afgesproken dienst, middel of product.
Kantoortijden: de periode waarin Leverancier bereikbaar is op de Werkdagen.
Klacht: (schriftelijke) uiting van ontevredenheid over de dienstverlening van Leverancier.
Leverancier: Onesurance.
Maintenance Window: tijdsperiode waarbinnen onderhoud gepleegd kan worden op de beheerde componenten.
Niet-Beschikbaarheid: de periodes waarin Acceptatie Assistent niet conform de afgesproken functionaliteit, zoals afgesproken in de dienstbeschrijving, toegankelijk is voor de geautoriseerde Gebruikers.
Norm: het percentage succesvolle incidentafhandelingen binnen de beloofde tijden waaraan Acceptatie Assistent minimaal moet voldoen.
Opdrachtgever: de klant van Onesurance.
Overeenkomst: de Overeenkomst en bijlagen
Overmacht: onvoorziene en onbeheersbare omstandigheden die buiten de controle van een Partij vallen en die de prestaties van de service negatief kunnen beïnvloeden. Voorbeelden zijn natuurrampen, terroristische activiteiten, stroomuitval, stakingen, of andere gebeurtenissen die buiten de redelijke controle van betreffende Partij liggen.
Partijen: Opdrachtnemer en Leverancier gezamenlijk te noemen “Partijen” en afzonderlijk te noemen “Partij”,
Partner: de klant van Leverancier, die de Diensten en/of applicatie van Onesurance afneemt.
Prioriteit: de mate van urgentie van het Incident, zoals beschreven in hoofdstuk 5.
Probleem: het niet voldoen door een in eerste instantie onbekende oorzaak wat kan leiden tot één of meerdere Incidenten.
Responsetijd: de tijd tussen het ontvangen van een melding en het moment dat deze wordt opgepakt (registratie, eerste contact met Opdrachtgever en start diagnose).
Recovery Point Objective (RPO): de maximale periode waarin dataverlies aanvaardbaar is bij een calamiteit.
Recovery Time Objective (RTO): de maximale tijd tussen een Incident en het weer beschikbaar zijn van de functionaliteit
Request for Change (RFC): een verzoek vanuit Opdrachtgever om een functionaliteit te wijzigen, toe te voegen of te verwijderen.
AI-as-a-Service: de applicatie van Onesurance die via internet beschikbaar wordt gesteld voor geautoriseerde Gebruikers.
Security breach: een Incident waarbij onbevoegden toegang krijgen tot data, applicaties, netwerken of apparaten zonder toestemming. Dit kan leiden tot Datalekken, verlies van vertrouwelijke informatie of andere negatieve gevolgen voor individuen of organisaties.
Support: het centrale aanspreekpunt van Leverancier voor de Gebruikers van Opdrachtgever.

Service Level: het door de leverancier te leveren niveau van een deelaspect van de Dienst(en), uitgedrukt door middel van een indicator.
Service Window: het tijdsbestek waarbinnen de Dienst(en) wordt/worden uitgevoerd.
Vergoeding(en): alle voor de Diensten overeengekomen Vergoedingen.
Werkdagen: een dag die valt binnen de Kantoortijden van Leverancier.
Wijziging: een verandering die uitgevoerd wordt op (onderdelen van) een Dienst of infrastructuur, met een (potentieel) zodanige impact dat aan de invoering een zorgvuldige beoordeling vooraf dient te gaan.

2. Algemeen AI-as-a-Service

Leverancier stelt haar AI-as-a-Service beschikbaar via internet en verzorgt het technisch onderhoud en het technisch beheer van de geleverde Diensten. Leverancier stelt haar producten beschikbaar vanuit een in EER gevestigd datacentrum. Om hier gebruik van te maken dient Opdrachtgever zorg te dragen voor een:

- ✓ Stabiele internetverbinding met snelheid van minimaal 5Mbps;
- ✓ Chromebrowser, voorzien van de laatste updates;
- ✓ Resolutie van minimaal 1600 x 900 in combinatie met een schaalgrootte 100%.

De Dienst is een AI-as-a-Service-applicatie en heeft daardoor de volgende voordelen en voorwaarden:

- ✓ Opdrachtgever hoeft de soft- en hardware waar deze software op is geïnstalleerd niet aan te schaffen, maar betaalt voor het gebruik van de AI-as-a-Service;
- ✓ Opdrachtgever heeft toegang tot de AI-as-a-Service via een beveiligde internetverbinding;

3. Technisch beheer door Onesurance

Het technisch onderhoud en beheer wordt door Leverancier verzorgd. Hieronder wordt verstaan het Infrastructuurbeheer, Gegevensbeheer, Beveiligingsbeheer, Naleving & audits en Performance-optimalisaties. Uiteraard verzorgt Leverancier ook de oplevering van nieuwe functionaliteiten in de applicatie.
Infrastructuur: Het beheren van de hardware-infrastructuur, zoals hosting, servers, en opslag, die nodig is om de AI-as-a-Service-toepassing te ondersteunen.
Gegevensbeheer: Het beheren van de gegevens die worden opgeslagen en verwerkt door de AI-as-a-Service-toepassing. Dit omvat het implementeren, beheren en controleren van Back-up- en herstelprocedures, het waarborgen van gegevensintegriteit en het voldoen aan nalevingsvereisten voor gegevensbescherming.
Beveiligingsbeheer: Het implementeren en onderhouden van beveiligingsmaatregelen om de AI-as-a-Service-toepassing te beschermen tegen bedreigingen zoals hackers, malware en Datalekken. Dit omvat het monitoren van beveiligingsgebeurtenissen, het uitvoeren van penetratietesten en het implementeren van toegangscontrolemechanismen.
Serviceondersteuning: Het bieden van technische ondersteuning aan de eindgebruikers van de applicatie. Het gaat hier om het aannemen van Incidenten, het in behandeling nemen van RFC's en eventueel het geven van betaalde trainingen.
Naleving en audits: Het voldoen aan wettelijke en industriële nalevingsvereisten zoals de AVG, en standaarden rondom informatie- en cyberbeveiliging. Daarnaast verleent Leverancier medewerking aan jaarlijkse audits en PEN-testen zodat de applicatie te allen tijde voldoet aan de geldende wet- en regelgeving.
Performancebehoud en -optimalisaties: Het beheren van de systemen en het identificeren van mogelijkheden voor het verbeteren van de prestaties van de AI-as-a-Service-toepassing, zoals het optimaliseren van code en verwerking van data.
Oplevering nieuwe functionaliteiten: Als er nieuwe functionaliteiten nodig zijn dan kan Opdrachtgever dit aangeven bij Leverancier en wordt dit door Leverancier tegen een overeengekomen gebouwd.
Functioneel beheer Leverancier is verantwoordelijk voor het functioneel beheer van de Dienst. Hieronder valt het Aannemen en verwerken van gebruikersvragen, Onderhouden van de inrichting, Periodieke checks verrichten op het functioneren van de inrichting, het aanleveren van data en requirements bij Opdrachtgever en het verzamelen van gebruikersfeedback.
Aannemen en verwerken van gebruikersvragen: De vragen die door eindgebruikers gesteld worden, moeten door de Leverancier aangenomen en verwerkt worden. Als de Opdrachtgever opmerkt dat iets een bug is dan kan dit bij Support

van Leverancier ingediend worden en wordt dit opgelost. Nieuwe functionaliteiten (RFC) kunnen ingediend worden via de Customer Success Manager. Generieke RFC's worden kosteloos geïmplementeerd, bij Partner specifieke vragen wordt een Vergoeding gevraagd die vooraf gecommuniceerd wordt.

Onderhouden van de inrichting: In het voorstel is een initiële inrichting van de applicatie door Leverancier opgenomen.

Aanleveren van data en requirements: Als Opdrachtgever data wil migreren, een nieuwe koppeling wil hebben of nieuwe functionaliteiten aanvragen, dan is Opdrachtgever verantwoordelijk voor het aanleveren van deze informatie. Voor koppelingen geldt dat Opdrachtgever verantwoordelijk is voor het opstellen van de requirements, het verzamelen van de benodigde informatie en credentials en het volledig testen en accorderen van de koppeling. Leverancier is niet verantwoordelijk voor eventuele fouten in een opgestelde en overeengekomen setup.

Verzamelen van gebruikersfeedback: Opdrachtgever is verantwoordelijk voor het verzamelen van de gebruikersfeedback. Met deze feedback zal Opdrachtgever de gebruikerservaring verbeteren door middel van een aanvraag van een RFC bij Onesurance.

Functionele ketentesten: Het is de verantwoordelijkheid van Opdrachtgever om regelmatig ketentesten uit te voeren, waarbij er getest wordt op de functionele werking van de applicatie en koppelingen. Deze ketentesten dienen als waarborg voor de kwaliteit van de inrichting en de integriteit van de data. Het doel hiervan is om ervoor te zorgen dat het systeem optimaal functioneert en voldoet aan de gestelde functionele eisen. Deze eisen zijn enkel door Opdrachtgever zelf te controleren, evenals de authenticiteit van de data.

4. Prestaties van de applicatie

Om goed met de AI-as-a-Service te kunnen werken is een snelwerkende applicatie erg belangrijk. Uiteraard is de snelheid afhankelijk van meerdere factoren, waaronder een goed werkend (Wi-Fi-) netwerk. Onder optimale omstandigheden streven we naar de volgende prestaties, exclusief gepland onderhoud en Overmacht, op basis van best-effort:

Type	Meetpunt	Meetmoment	Norm prestatie	Norm
Beschikbaarheid	Uptime percentage	Maandelijks	95% bereikbaarheid	90%
Snelheid	Frontend laadtijd	Bij het laden van een pagina	3 sec	90%
Capaciteit	Aantal gelijktijdige gebruikers	Tijdens piekbelasting	Max 50 gebruikers	90%
Hersteltijd	Tijd om kritieke storingen op te lossen	Na een kritieke storing	48 uur	90%

Het is de verantwoordelijkheid van Opdrachtgever om ervoor te zorgen dat de omgeving regelmatig wordt opgeschoond en bijgehouden, zodat onnodige gegevens worden verwijderd en het systeem optimaal presteert zonder vertragingen als gevolg van overbelasting of overbodige informatie waardoor bovenstaande tijden niet gehaald zouden worden.

5. Beschikbaarheid productieomgeving AI-as-a-Service

Leverancier committeert zich aan een Beschikbaarheid van ten minste 95% voor haar AI-as-a-Service, verminderd met de Geplande Niet-Beschikbaarheid. De afgegeven prestatie indicatoren hebben betrekking op dienst(en) van Leverancier in een productieomgeving en gelden niet voor Diensten in een acceptatieomgeving. De Beschikbaarheid wordt berekend per kalendermaand volgens de formule:

Uptime = { (T – D) / T } * 100%
T: Service Window per maand
D: Totale Niet-Beschikbaarheid (Downtime)
- Downtime in een Maintenance Window, wordt in de berekening buiten beschouwing gelaten.

Onze uitgangspunten rondom Beschikbaarheid zijn:

1. Werkzaamheden die impact hebben op de Beschikbaarheid van de AI-as-a-Service worden zoveel mogelijk buiten Kantoortijden uitgevoerd, over dit onderhoud zal Leverancier Opdrachtgever uiterlijk 7 dagen vooraf schriftelijk informeren. In uitzonderlijke situaties kan het voorkomen dat Leverancier deze werkzaamheden binnen Kantoortijden moet uitvoeren, dit wordt alleen in het geval van een hoge prio gedaan en na overleg met Opdrachtgever.
2. Niet-Beschikbaarheid als gevolg van onderstaande redenen en oorzaken kan niet aan Leverancier worden toegerekend en valt derhalve buiten de Beschikbaarheid:
   a) Met Opdrachtgever schriftelijk overeengekomen onderhoudswerkzaamheden tijdens het Maintenance Window
   b) Incidenten als gevolg van Overmacht.

6. Beschikbaarheid acceptatieomgeving AI-as-a-Service

Indien gewenst door Opdrachtgever verzorgt Leverancier de mogelijkheid om een acceptatieomgeving in te richten. Dit wordt tijdens de projectfase besproken en zo nodig ingericht door Leverancier, bij wie tevens de verantwoordelijkheid rust om de omgeving te onderhouden. Leverancier committeert zich aan een Beschikbaarheid van de acceptatieomgeving van ten minste 85% voor haar AI-as-a-Service, verminderd met de Geplande Niet-Beschikbaarheid. De Beschikbaarheid van de acceptatieomgeving is lager dan de productieomgeving omdat er regelmatig testscenario's voor onze Partners uitgerold worden, zodat er uitvoerig getest kan worden voordat items naar productie gaan. De afgegeven prestatie indicatoren hebben betrekking op dienst(en) van Leverancier in een acceptatieomgeving en gelden niet voor Diensten in een productieomgeving. De Beschikbaarheid wordt berekend per kalendermaand volgens de formule:

Uptime = { (T – D) / T } * 100%
T: Service Window per maand
D: Totale Niet-Beschikbaarheid (Downtime)
- Downtime in een Maintenance Window, wordt in de berekening buiten beschouwing gelaten.

De uitgangspunten rondom Beschikbaarheid voor de acceptatieomgeving zijn:

1. De acceptatieomgeving wordt na overleg en volgens afspraak bijgewerkt met de nieuwe functionaliteiten.
2. Indien een update eerder doorgevoerd moet worden dan wordt dit besproken en in overleg uitgevoerd op een tijdstip waarop de impact voor Opdrachtgever minimaal is.
3. Belangrijke updates worden overdag uitgevoerd nadat Opdrachtgever hiervan tijdig in kennis is gesteld en zo nodig maatregelen heeft kunnen treffen, indien noodzakelijk, als resultaat kan de applicatie tijdelijk niet beschikbaar zijn.

7. Meten van de Beschikbaarheid

Om de Beschikbaarheid proactief te kunnen meten maakt Leverancier gebruik van:

- Monitoring van de servers om te meten of deze actief zijn;
- Monitoring van de AI-as-a-Service op activiteit en belasting van de omgeving;
- Aantal succesvolle logincontroles op de AI-as-a-Service;

Uitgangspunten bij de inlogcontrole:

- Inlogcontrole gaat uit van één inlogpoging per minuut binnen het Service Window;
- Inlogpogingen tijdens het Maintenance Window worden genegeerd.

Op verzoek kan er een uitdraai gemaakt worden van de niet gevoelige informatie zoals de Beschikbaarheid in percentage.

8. Monitoring van de omgeving

Onze AI-as-a-Service-oplossingen en bijbehorende portalen worden net als de infrastructuur 24x7 gemonitord. Indien er verstoringen ontstaan in de onderliggende infrastructuur of op de applicatie ontvangt het Leverancier een geautomatiseerde melding. Leverancier tracht de verstoring direct te verhelpen. Service Window
Leverancier garandeert binnen het Service Window een Beschikbaarheid volgens de onderstaande Norm.

Omschrijving	Beschikbaarheid	Opmerking
Service Window	8:30 – 17:30 ma t/m vrijdag	Exclusief Maintenance Window
Maintenance Window	Aangekondigd en gepland	Indien noodzakelijk met vooraankondiging
Norm Beschikbaarheid	95%	Per maand binnen het Service Window

Het Maintenance Window stelt Leverancier in staat op vooraf vastgestelde tijdsvensters gepland onderhoud uit te voeren.

Omschrijving	Beschikbaarheid	Opmerking
Maintenance Window	Aangekondigd en gepland	Mogelijke impact op Beschikbaarheid of prestatie*

*Onderhoud met impact op de Beschikbaarheid wordt minimaal 7 Werkdagen vooraf schriftelijk aangekondigd, tenzij er sprake is van een beveiligingsincident en/of urgente Wijziging. In het laatste geval neem Leverancier hier zo snel mogelijk contact op met de contactpersoon van Opdrachtgever. Als er voorzien wordt dat er door een urgente Wijziging een conflict kan ontstaan met regulier onderhoud in het Maintenance Window, dan zal Leverancier als eerste de urgente Wijziging uitvoeren en indien mogelijk daarna het regulier onderhoud. Indien het niet mogelijk is om het regulier onderhoud uit te voeren wordt er voor dit regulier onderhoud een ander moment gepland. De Prioriteit ligt te allen tijde bij het doorvoeren van de urgente Wijziging. Om de dienstverlening te garanderen is het van belang om relevante updates tijdig door te voeren. Leverancier voert de nieuwe security updates daarom door volgens onderstaande termijn.

Rating	Doorlooptijd	Uitleg
Niet kritisch	< 3 maanden	Een (security) Incident dat zich voordoet waarbij er geen bedrijfsimpact
Medium Prioriteit	< 1 maand	Een (security Incident dat zich voordoet waarbij de bedrijfsimpact miniem en er geen risico bestaat op datalekken.
Hoge Prioriteit	Per direct, < 72 uur	Een (security) Incident dat zich voordoet waarbij een bedrijfsimpact mogelijke is.
Kritiek	Per direct, < 48 uur	Een (security) Incident dat zich voordoet waarbij een bedrijfsimpact aanzienlijk is.

9. Verantwoordelijkheden testen na maintenance

Leverancier is verantwoordelijk voor de uptime van de applicatie en de techniek. Na maintenance zal Leverancier daarom een check doen op de werking van de functionaliteiten. Als er in de inrichting van de applicatie Wijzigingen worden doorgevoerd dan wordt Opdrachtgever hiervan per e-mail vooraf op de hoogte gesteld. Het is de verantwoordelijkheid van de Leverancier om na een update een functionele test uit te voeren om te controleren of functionaliteit nog werkt zoals initieel is bedoeld. Koppelingen wordt niet aangepast zonder wederzijdse toestemming (indien de werking van de koppeling verandert) en vallen derhalve buiten de scope voor het testen na maintenance. Het updaten van de acceptatieomgeving, het testen en de release naar productie gebeurt altijd op basis van vooraf gecommuniceerde planning van Leverancier.

10.Ondersteunende diensten

Supportverzoeken

Leverancier biedt ondersteuning op haar AI-as-a-Service. Hiervoor is Support van Leverancier beschikbaar voor het beantwoorden en afhandelen van serviceverzoeken (Calls). Serviceverzoeken mogen enkel aangemeld worden door de projectbegeleiding van Opdrachtgever. De telefonische bereikbaarheid voor deze ondersteuning is tijdens Kantoortijden.

Service Desk dienst	Dagen	Periode
Support: +31 6 132 70 144	Ma t/m vr*	08:30-17:30 uur

**uitgezonderd Feestdagen*

Meldingen die worden geplaatst worden binnen de Kantoortijden opgepakt op basis van Prioriteit. De Prioriteit wordt in eerste instantie opgegeven door Opdrachtgever, waarbij Leverancier de mogelijk heeft om de Prioriteit aan te passen. Partijen kunnen, op verzoek van Opdrachtgever, overeenkomen om tijdelijk af te wijken van de Kantoortijden en extra Beschikbaarheid in te kopen, zoals tijdens het uitvoeren van projecten en/of releases.

11.Scope en typen Calls

Het soort Call dat primair onder de SLA valt en waar de voorwaarden van de SLA op van toepassing zijn is een Incident. Dit is een fout in de software, koppeling of data wat de normale werking van de Dienst verstoort of ongewenste resultaten oplevert. Hierin zijn drie categorieën:

- Incidenten, het verhelpen hiervan;
- Privacy- en security Incidenten en (ver-)storingen;
- Correctieverzoeken, corrigeren van beschadigde data of koppelingen waarbij de oorzaak bij Leverancier ligt.

Secundaire Calls vallen niet onder de SLA-voorwaarden maar worden wel door Leverancier in behandeling genomen. Hieronder valt:

- Restore verzoeken, terugzetten van Back-ups.
- Vragen, beantwoorden van vragen vanuit functioneel beheer;
- Consultancy, inhuur voor trainingen;
- Request for Changes (RFC's), verzoek tot aanpassingen van de programmatuur;
- Alle overige vragen en/of verzoeken die geen directe relatie hebben tot de AI-as-a-Service.

Opdrachtgever geeft bij het aanmelden van een Call aan welk soort Call het betreft. Het is aan Leverancier om dit te controleren en zo nodig te wijzigen. Secundaire calls zijn normaliter betaalde opdrachten, afgezien van RFC's die generiek gebouwd kunnen worden door Leverancier. Het verzoek tot terugzetten van een Back-up waarbij de toedracht van de noodzaak van een Back-up niet bij Leverancier ligt is ook een betaalde opdracht.

12. Klachten en communicatiematrix

Indien er Klachten zijn over de dienstverlening kunnen deze doorgegeven worden aan de toegewezen Customer Success Manager van Leverancier. Support registreert de Klacht en wijst die toe aan een behandelaar. Opdrachtgever wordt op de hoogte gehouden van de voortgang. Na Acceptatie van het klachtrapport door Opdrachtgever wordt de melding als opgelost beschouwd en wordt de melding gesloten. Indien men er niet uitkomt en/of indien de Klacht gevoelig ligt kan deze besproken worden in een hoger echelon. Een escalatie kan worden gemeld bij de Customer Succes Manager van Leverancier op het moment dat een melding niet naar tevredenheid wordt opgepakt/opgelost. Als er aanleiding is om naar een ander niveau te escaleren kan dat volgens het onderstaande communicatiemodel.

13. Incidentmanagement

Het doel van incidentmanagement is ervoor te zorgen dat de Acceptatie Assistent zo snel mogelijk weer operationeel is. Incidentmanagement gaat niet over het oplossen van de oorzaak.

- De Incidenten worden op basis van Prioriteit en doorlooptijd afgehandeld. Incidenten met een hogere Prioriteit hebben altijd voorrang;
- Een Incident geldt als opgelost indien Leverancier een (tijdelijke) oplossing realiseert die de overeengekomen werking herstelt.

De volgorde van afhandeling van Incidenten die bij Leverancier gemeld worden, wordt door Leverancier bepaald met inachtneming van de in dit hoofdstuk omschreven prioriteitstelling. Het kan voorkomen dat Leverancier een Incident eerder opmerkt dan Opdrachtgever. Als het een Prioriteit 1 Incident betreft, stelt Leverancier haar Partners hiervan onverwijld via een schriftelijke melding op de hoogte. Indien dit langer dan 4 uur aanhoudt zal er via de e-mail een update komen, inclusief een verslag over de oorzaak en de oplossing.
Opdrachtgever kan bij het aanmelden van een Incident een urgentieniveau meegeven. Bij het melden van een urgentie “prio 1” dient u deze telefonisch kenbaar te maken bij Support, alvorens een schriftelijke melding te sturen naar support@onesurance.nl. Dit om ervoor te zorgen dat er sprake is van een “warme” overdracht, waardoor ook direct de urgentie bekend is binnen Leverancier. De Normen rondom urgentie zijn hieronder opgenomen:

Omschrijving	Urgentie	Voorbeeld
Prio 1	Kritiek	De Diensten zijn niet meer te gebruiken en een workaround is niet mogelijk.
Prio 2	Hoog	Normale uitvoering van een deel van de Dienst is niet mogelijk, impact is aanzienlijk.
Prio 3	Middel	De Diensten werken niet volledig maar er is geen verdere bedrijfsimpact.
Prio 4	Laag	Een Incident dat zich voordoet waarbij er geen bedrijfsimpact is.

De melder kan de Prioriteit van het Incident doorgeven, deze wordt door Support gecheckt op basis van bovenstaande voorwaarden en geconformeerd of aangepast.

14.Respons- & Afhandeltijd

Voor een prio 1 Incident geldt dat Leverancier voor een structurele oplossing zorgdraagt, dan wel een voor Opdrachtgever acceptabele workaround te realiseren. Dit houdt in dat Leverancier zich aan de inspanningsverplichting houdt tot de functionaliteit weer normaal beschikbaar is, of de urgentie is afgeschaald naar prio 2 of 3.
Voor prio 2 en 3 kan Leverancier besluiten om verdere afhandeling van een Call conform planning af te handelen. Dit wordt gemeld in de afhandeling van de Call d.m.v. een planning. Dit is bijvoorbeeld het geval bij bug fixes in applicatie en/of interfaces.
Leverancier hanteert de onderstaande criteria en doorlooptijden m.b.t. het afhandelen van de Incidenten. Zodra duidelijk is dat de oplossing van een Incident niet binnen de afgesproken oplostijd kan worden gerealiseerd neemt Leverancier, in overleg met de melder, de beslissing om de escalatieprocedure te starten.

Prioriteit	Responsetijd	Afhandeltijd	Norm
Prio 1: kritiek (tijdens Kantoortijden)	< 60 minuten	< 48 uur	95%
Prio 2: hoog (tijdens Kantoortijden)	< 4 uur	< 72 uur	95%
Prio 3: middel (tijdens Kantoortijden)	< 1 Werkdag	< 20 Werkdagen*	95%

** Prio 3 bugs worden in de regel sneller opgelost, maar wanneer er ontwikkelwerk nodig is dan wordt dit op de volgende sprint ingepland en opgeleverd. Daarbij is de uiterlijke doorlooptijd 20 Werkdagen.*
Voor items lager dan een prio 3 geldt geen Afhandeltijd aangezien dit geen blokkerende issues zijn. In de regel gaan deze items mee in de ontwikkelsnelheid van Incidenten met prio 3.

15. Wijzigingsbeheer

Wijzigingen binnen de omgeving van Acceptatie Assistent zijn ingericht in 3 categorieën:

1. Wijzigingen om Acceptatie Assistent te optimaliseren op functioneel en/of technisch vlak wordt geïnitieerd door Leverancier. Dit zijn Wijzigingen met als doel om functionaliteiten toe te voegen aan de omgeving en/of om Problemen weg te nemen;
2. Calls die wordt geclassificeerd als RFC om op verzoek van Opdrachtgever een aanpassing door te voeren, dit kan zijn een functionaliteit toe te voegen of aan te passen, maar ook om een restore uit te voeren;
3. Standaard Wijzigingen, dit zijn aanpassingen die geen impact hebben op de bestaande functionaliteit.

Ook Wijzigingen mogen alleen door de projectbegeleiding van Opdrachtgever worden ingediend. Indien er kosten gemoeid zijn met de aanpassing, zal Leverancier de Wijziging pas uitvoeren na schriftelijk akkoord van Opdrachtgever. Het indienen van Wijzigingen dient via de Servicedesk te gebeuren zoals in hoofdstuk ‘4.1 Supportverzoeken’ is beschreven. Het changeproces na ontwikkeling is hieronder in hoofdstuk ‘5.3 Software release’ opgenomen.

16. Software release

Leverancier maakt gebruik van continuous integration, waardoor er een mogelijkheid is om opgeleverde changes, die een hogere urgentie hebben, direct naar de productie omgeving over te zetten. Minder urgente changes die opgeleverd worden, zullen conform vooraf gemaakte afspraken worden opgeleverd. Bij het opleveren van een release, geeft Leverancier tot maximaal 1 week na de release releasedocumentatie vrij. In deze documentatie staat beschreven wat de, voor Opdrachtgever, relevante aanpassingen zijn die opgenomen zijn in de volgende release. Na de software release voert Leverancier testen uit, maar van de Partner wordt ook verwacht dat zij testen op de Acceptatie-omgeving indien aanwezig, en na de release op de Productie-omgeving. Het is mogelijk bij Leverancier nieuwe functionaliteit of een software aanpassing aan te vragen. Dit kan door middel van het aanmelden van een Request for Change (RFC) bij de Customer Success Manager. De Customer Success Manager geeft ook terugkoppeling op het verzoek of het is goedgekeurd, of is afgewezen.

17. Wettelijke vereisten

Leverancier is gehouden aan wet- en regelgeving. We passen onze software hier tijdig op aan, zodat ook Opdrachtgever hier tijdig aan kan voldoen. Deze wettelijke Wijzigingen worden door een softwarerelease uitgeleverd in de AI-as-a-Service.

18. Probleem management

Het doel van probleem management is het verminderen van de waarschijnlijkheid en impact van Incidenten door actuele en potentiële oorzaken van Incidenten te identificeren, en workarounds en known errors te managen.
Probleem identificatie wordt gestart vanuit de volgende situaties:

1. Alle meldingen die betrekking hebben op Incidenten en niet direct opgelost kunnen worden, maar waar wel een workaround voor beschikbaar is, worden gekwalificeerd als Probleem;
2. Incidenten die frequenter optreden maar niet direct opgelost kunnen worden en waar geen workaround voor beschikbaar is worden als Probleem gekwalificeerd;
3. Leverancier analyseert periodiek het aantal meldingen dat binnenkomt, zowel vanuit Opdrachtgever als vanuit de interne monitoring. Door de meldingen te classificeren en te groeperen herkent de AI-as-a-Service trends. Deze trends kunnen wijzen op structurele Problemen/onduidelijkheden voor Opdrachtgever en/of in de techniek. Op basis van

deze trends onderzoekt Leverancier de oorzaak en komt met een structurele oplossing. De oplossing komt terug in een volgende release;

4. Leverancier is verantwoordelijk voor het realiseren van een workaround, Opdrachtgever is verantwoordelijk voor het testen en Accepteren van de workaround.

19. Security en hosting

Veiligheid Leverancier doet het uiterste om haar Diensten veilig te houden door middel van beveiligingsmaatregelen. Dit doet Leverancier van infrastructuur tot applicatie. In het geval van een Security breach behoudt Leverancier zich het recht voor de AI-as-a-Service per direct uit te schakelen om eventuele schade te beperken. Leverancier doet al het mogelijke om de oorzaak te achterhalen en op te lossen. Leverancier logt hier een prio kritiek Incident voor en handelt dit ook conform dit proces af.

Securitytesten Indien Opdrachtgever security testen wenst uit te voeren op de AI-as-a-Service, dient Opdrachtgever hiervoor toestemming te vragen aan Leverancier. Dit vraagt Leverancier om te voorkomen dat bij haar onverklaarbare notificaties volgen, waardoor ze maatregelen kunnen nemen die schadelijk zijn voor de continuïteit van een of meerdere klanten. In overleg kan de test worden ingepland. Leverancier zal in alle gevallen medewerking verlenen aan dergelijke verzoeken. De kosten voor securitytesten worden gedragen door Opdrachtgever. De samenvatting hiervan wordt gedeeld en is ook op verzoek per mail te verkrijgen. Daarnaast is er een actief 4-ogen principe op alle code dat naar de productie-omgeving gaat.

Dataverwerking Leverancier verwerkt, als verwerker, nooit data voor doeleinden anders dan afgesproken en waarvoor een wettelijke grondslag bestaat. Bovendien wordt er door Leverancier nooit data opgeslagen op locaties buiten de Europese Unie. Dit geldt zowel voor de hosting als de disaster recovery locatie.

De Dienst worden gehost bij Microsofts Azure Clouddiensten. Deze zijn door Leverancier in de verwerkersovereenkomst aangemerkt als sub-verwerker. Voor meer informatie over Microsofts Azure certificeringen, zie https://learn.microsoft.com/en-us/azure/compliance/.

20. Redundantie en Back-up

Voor Back-ups maakt Onesurance gebruik van het Back-up beleid zoals verzorgd door Microsoft Azure. Meer informatie over dit beleid is te vinden op: https://learn.microsoft.com/nl-nl/sql/relational-databases/Back-up-restore/backup-overview-sql-server?view=sql-server-ver16. Leverancier is verantwoordelijk voor het maken van database Back-ups en het toetsen op integriteit. Back-ups van het primaire datacenter worden uitgevoerd volgens onderstaand schema:

Soort Back-up	Omgeving	Soort	Frequentie	Bewaartermijn
Database	Productie	Full	Dagelijks	1 week
	Productie	Differential	Elke 24 uur	4 weken
	Productie	Transactional	Elke 10 min.	3 maanden

De Back-up wordt vervolgens op de onderstaande manier behandeld:

Dienst	Service Level
Archivering locatie	Op basis van Zone Redundant Storage
Back-up window	Buiten Kantoortijden

Redundantie	Er wordt geen verwerkte data opgeslagen aan de kant van Onesurance. In het geval van een kritieke situatie wordt de hosting voor de API opnieuw opgezet en uitgerold, of een recente Back-up van deze omgeving restored.
RPO	8 werkuren
RTO	24 uur
Locatie	**Adres**
MS West Europe	Cultuurweg 11, 1775 RA Middenmeer, Nederland

Om zeker te zijn dat de omgeving te herstellen is voert Leverancier periodiek (1x per jaar) een full recovery herstelactie uit. Om zeker te zijn dat de omgeving na de herstelactie functioneel bruikbaar is betrekt Leverancier hier een of meerdere Partners bij. Van deze actie wordt ook een verslag gemaakt, waardoor het voor al de Partners van Leverancier en eindklanten en audit aantoonbaar is dat we deze actie hebben uitgevoerd. Dit zal verder besproken worden tijdens de tactische overleggen.

21. Technische architectuur

AI-as-a-Service-omgevingen worden uitgerold met een combinatie van een aantal Azure tools:

- Azure DevOps (voor het orkestreren van het proces van code naar applicatie in de cloud);
- Azure Machine Learning (voor het opslaan van het model);
- Azure App Service (voor het hosten van de API) en Terraform (voor het definiëren van de Azure infrastructuur in code templates). De code is te vinden in Azure DevOps.

Om aanpassingen aan het model en de API op een veilige manier te kunnen testen, zijn er twee endpoints (URL's) voor de API waarvan gebruik gemaakt kan worden. Dit is een functionaliteit van Azure App Service, genaamd "deployment slots". Hiermee kunnen eenvoudig twee versies van het model naast elkaar in de cloud gedraaid worden.

22. Monitoring, detectie

Leverancier heeft actieve monitoring en detectie op zowel servers als software. Dit betekent dat er actief toezicht wordt gehouden op mogelijke oneigenlijke inlogpogingen door kwaadwillende. Bij onregelmatigheden wordt geautomatiseerd per ommegaande een waarschuwing verstuurd naar Support. Deze waarschuwingen worden altijd als een Prio 1 Incident beschouwd, waardoor er direct gepaste actie kan worden ondernomen.

23. Informatiebeveiliging

Informatiebeveiliging is een belangrijk onderdeel binnen Leverancier. Omdat er gevoelige informatie opgeslagen en verwerkt wordt hebben wij een aantal belangrijke processen om de integriteit van de data te kunnen waarborgen.

24. Structuur informatiebeveiliging

Leverancier is actief bezig met informatiebeveiliging en de controle hierop. Zowel voor het onderhoud van de applicatie als de bedrijfsvoering zijn er een aantal verantwoordelijken die hierop toezien en controleren. De Data Protection Officer rol is een uitvoerende en interne rol. De Data Protection Officer zorgt voor een juiste Implementatie van en toezicht op geldende wet- en regelgeving en daaruit voortkomende verplichtingen. De Data Protection Officer adviseert het management van Onesurance en schrijft samen met hen het informatiebeveiligingsbeleid. Deze rol omvat binnen Onesurance ook de controle op de uitvoering van het beleid in de organisatie en uitvoering.

25. Data-incidenten

Wanneer er een vermoeden is van een Datalek wordt direct de Data Protection Officer ingeschakeld. De Data Protection Officer onderzoekt het gemelde Incident samen met de Heads of Engineering en Machine Learning en koppelt via Support, binnen 24 uur na het vermoeden van een Datalek, terug aan Opdrachtgever of er sprake is van een Datalek. Als dit het geval is wordt er een Incidentrapport (zie hoofdstuk 7.3) opgesteld en worden indien nodig de betrokken instanties op de hoogte gebracht. Er wordt een uitgebreide verslaglegging gedaan en Leverancier zal diepgaand onderzoek uitvoeren om de oorzaak te achterhalen, verbeterpunten op te stellen en een actieplan te maken waarin wordt omschreven hoe vergelijkbare situaties in de toekomst voorkomen worden. Er zal na het afdichten van het Datalek direct gestart worden met de uitvoering van dit actieplan

26. Incidentrapport

Wanneer er sprake is van een Datalek wordt een incidentrapport opgesteld en gedeeld met de melder van het Incident en met alle bij het Incident betrokken stakeholders. Een incidentrapport bestaat uit de verslaglegging van het Probleem, de oorzaak, de impact en de oplossing. Het Probleem wordt zo snel mogelijk verholpen en de ontvangers van het incidentrapport worden op de hoogte gehouden. De Functionaris Gegevensbescherming ziet toe op een juiste afhandeling, het oplossen van het Incident en de nazorg. In de nazorg doet Leverancier onderzoek naar mogelijkheden om te voorkomen dat een dergelijke situatie zich opnieuw voordoet en zal dit melden bij in het incidentrapport.

27. OTAP-straat

Indien overeengekomen met Opdrachtgever, zal Leverancier gebruik maken van de OTAP-methodiek voor de softwareontwikkeling. Op deze manier wordt er een duidelijk onderscheid gemaakt in de verschillende omgevingen. Het ontwikkelteam werkt in de ontwikkelomgeving, Leverancier consultants testen in de testomgeving, de Partner test in de acceptatieomgeving en de Gebruikers werken in de productieomgeving. Er wordt gebruik gemaakt van gesplitste omgevingen en databases, zodat er geen data Incident kan ontstaan door mengeling van data door de verschillende omgevingen heen.