otherside at work
for happy professionals

SERVICE LEVEL AGREEMENT
XPERT SUITE

AUTEUR Rob Brekelmans

FUNCTIE Manager Customer Operations

VERSIE 5.10

STATUS Definitief

DATUM 16 september 2021

CLASSIFICATIE Gevoelig

powered by
fair priced technology

INHOUDSOPGAVE

ALGEMEEN

1.1 JURIDISCHE KOPPELING MET OVEREENKOMST & CHANGE MANAGEMENT SLA

Opdrachtgever en Otherside zijn een Overeenkomst aangegaan ten behoeve van de service en dienstverlening. Tussen betrokken Partijen is de Overeenkomst leidend en dit Service Level Agreement (SLA) is een uitwerking van het ondersteunings- en onderhoudselement in het kader van de Xpert Suite Software en Diensten die als Software as a Service (SaaS) oplossing aangeboden wordt.

Ingangsdatum van de SLA is de go-live datum van de software. De verplichtingen in deze SLA stoppen wanneer de Overeenkomt tussen Opdrachtgever en Otherside eindigt.

1.2 SCOPE VAN DE DIENSTVERLENING

Partijen streven naar een langdurige relatie betreffende de ontwikkeling van bedrijfsgezondheid- & verzuimprocessen met behulp van de SaaS-oplossing Xpert Suite. De in dat kader overeengekomen dienstverlening heeft betrekking op het exploiteren van Xpert Suite, het verlenen en uitvoeren van ondersteuning en onderhoud, waaronder de verdere ontwikkeling van Xpert Suite, alsmede de daarmee samenhangende werkzaamheden zoals vastgesteld in de Overeenkomst en deze SLA. Deze diensten worden geleverd op het in dit SLA overeengekomen Service Level. De SaaS-oplossing Xpert Suite bestaat uit de volgende dienstverlening:

- Exploitatie:
  - Continuïteits-, capaciteits- & beschikbaarheidsmanagement;
- Servicedesk; Xpert Desk: ondersteuning van het applicatiebeheer van de Opdrachtgever:
  - Incidentmanagement;
  - Change management;
- Strategische release ontwikkeling:
- Versiebeheer en deployment:
  - Release management.

Naast de diensten die worden geleverd door de Xpert Desk, kan Otherside ook diensten leveren voor eerstelijnsondersteuning en functioneel beheer onder regie van de Opdrachtgever. Deze aanvullende diensten zouden kunnen worden overeengekomen door ondertekening van een addendum genaamd Functioneel Applicatiebeheer. Een vaste capaciteit per maand wordt toegewezen aan de Opdrachtgever en wordt uitgevoerd door professionals van Otherside die hiervoor zijn opgeleid en die de vaardigheden bezitten om de taken uit te voeren die in het addendum worden beschreven. Eerstelijnsondersteuning en functioneel beheer vallen niet onder de SLA.

1.3 SERVICEDESK; XPERT DESK

De functioneel applicatiebeheerder van Opdrachtgever voert eerstelijns servicedeskactiviteiten uit voor de gebruikers van Opdrachtgever. Functionele- en technische vragen over de werking van Xpert Suite kunnen alleen door de functioneel applicatiebeheerder en enkele key users van de Opdrachtgever (Super Users in Xpert Suite) worden gesteld bij de servicedesk van Otherside; **Xpert Desk**. Vragen en verstoringen worden conform in deze SLA vastgestelde reactie- en oplostijden afgehandeld. De Xpert desk van Otherside is bereikbaar binnen de in de SLA vermelde openingstijden. De Opdrachtgever is voor het raadplegen van de Xpert desk van Otherside geen extra kosten verschuldigd (dit is onderdeel van het software tarief), tenzij anders vermeld.

De Xpert desk van Otherside registreert en bewaakt de afhandeling van alle incidenten en wijzigingen en rapporteert hierover. Per ingangsdatum contract stelt Otherside aan de "Xpert Suite Super Users" van de Opdrachtgever toegang tot de servicemanagementapplicatie van Otherside beschikbaar, zodat de bevoegde functionarissen van de Opdrachtgever de incidenten en wijzigingen daarin rechtstreeks kunnen registreren, waarna Otherside conform de afgesproken Service Levels de incidenten en wijzigingen zal verwerken en bewaken.

1.3.1 BEREIKBAARHEID

Aanmelden van Functionele Vragen, Serviceverzoeken (bv. verzoek om herstelacties, database kopie maken etc.), Productsuggesties, Bugs en Storingen kan geschieden:

- via de servicemanagementapplicatie van Otherside (aanbevolen voor incidenten met prioriteit 3 en 2 en wijzigingen):

Als Super User toegang via Xpert Suite toepassing	

- per e-mail:

24 uur / 7 dagen per week	xpertdesk@othersideatwork.nl

- per telefoon (aanbevolen voor tickets met prioriteit 1):

Tijdens kantoortijden maandag t/m vrijdag 8:30 – 17:30	+31 73 6159999

- per e-mail met prioriteit (alleen voor tickets met prioriteit 1), de dienstdoende technicus zal binnen een uur reageren:

Buiten kantoortijden en feestdagen	storingen@othersideatwork.freshdesk.com

1.4 DATA & BEVEILIGING

1.4.1 INFORMATIEBEVEILIGING

Otherside hecht zeer veel waarde aan de beveiliging van de gegevens van haar opdrachtgevers. De hoge eisen die wij hieraan stellen komen tot uiting in zowel fysieke, technische alsook procedurele maatregelen welke wij zowel intern als bij onze leveranciers voorschrijven, naleven en controleren.

De beveiligingsaanpak van Otherside behelst:

1 Inbedding informatiebeveiliging in de organisatie;

2 Logische en fysieke toegangsbeveiliging;

3 Functioneel beheer, verbindingen en hosting;

4 Monitoring en verbetering beveiligingsmaatregelen & -incidenten;

5 Softwareontwikkeling;

6 Back-up & restore procedures.

Otherside is in het bezit van een ISO 27001:2013 certificaat en kan tevens een ISAE 3402 Type II verklaring overleggen. Hiermee is het managementsysteem waarmee Otherside de risico's rondom de beschikbaarheid en beveiliging van Xpert Suite beheerd volgens deze internationale standaard geauditeerd, gecertificeerd en geaccrediteerd.

De informatiebeveiliging wordt beheerst via het ISO 27001 gecertificeerde Information Security Management Systeem (ISMS), geregistreerd via BSI Group onder certificaatnummer ISC-077. De beheerder hiervan is de 'security officer' die tevens directielid is. Het managementsysteem maakt integraal onderdeel uit van de (jaarlijkse) besturingscyclus van het bedrijf als geheel:

- Ieder jaar wordt een risicoanalyse uitgevoerd op basis van de ervaringen van het afgelopen jaar en ontwikkelingen in de omgeving;
- Op basis van de risicoanalyse worden verbeterplannen gemaakt die ter goedkeuring aan het directieteam worden overlegd;
- Na goedkeuring wordt uitvoering van deze verbeterpunten door het MT integraal in de sturing van het bedrijf bewaakt.

Naast het managementsysteem zijn er beheersprocessen ingericht waar afzonderlijke verantwoordelijken sturing op geven. Elk proces kent een eindverantwoordelijke die, in samenspraak met de directie, bepaalt wanneer en waarop controles plaatsvinden. Of elke verantwoordelijke ook daadwerkelijk zijn rol pakt wordt tenslotte gecontroleerd in de jaarlijkse interne en externe ISO-audit. De ingestelde controls/maatregelen, zoals benoemd in ISO 27002, zijn allen in beheer en worden gecontroleerd. De volgende beheersprocessen zijn ingericht:

1 Asset & change management (incl. sleutelbeheer – Encryptie);

2 Patch management & hardening;

3 Capaciteitsmanagement;

4 Toegangsmanagement;

5 Incidentmanagement;

6 Beheer derde partijen;

7 Personeelsmanagement;

8 Compliance management;

9 Continuïteitsmanagement;

10 Klantenmanagement.

Binnen het personeelsmanagement is expliciet aandacht voor:

- Awareness op het gebied van informatiebeveiliging; Er worden meerdere keren per jaar kennisavonden gehouden over het belang van informatiebeveiliging voor onze opdrachtgevers en het voortbestaan van ons bedrijf. Tevens worden periodiek posters en andere visuele middelen gebruikt om mensen op procedures te wijzen. Voorbeelden hiervan zijn de lijsten die bij de papierbak en de printer hangen van welke spullen wel en welke niet hierin weggegooid dan wel geprint mogen worden. Ook in het personeelshandboek zijn diverse richtlijnen rondom informatiebeveiliging opgenomen en wordt actief gewezen op het informatiebeveiligingsbeleid. Bij het creëren van awareness op het gebied van informatiebeveiliging worden naast procedures ook potentiële grote gevolgen van

verkeerd handelen getoond. Deze gevolgen hebben betrekking op de personen en opdrachtgevers waarover informatie in onze systemen vastligt. Dit heeft als doel medewerkers niet alleen te motiveren om puur de procedures te volgen, maar ook om altijd zelf kritisch te blijven nadenken of er handelingen worden verricht die voor onze Opdrachtgever(s) en dus ook voor Otherside zelf grote nadelige gevolgen kunnen hebben.

- Competenties; Er wordt actief beoordeeld, bij indiensttreding en daarna elk jaar, of competenties van medewerkers aansluiten bij de functie die zij hebben of dat hier ontwikkeling in nodig is. Wanneer competenties niet meer aansluiten bij de functie, is een wijziging van functie een mogelijkheid. Bij personele wijzigingen wordt actief beoordeeld of de juiste competenties nog in het bedrijf aanwezig zijn of dat er gaten ontstaan. Wanneer het laatste het geval is, wordt gekeken hoe deze competenties binnen de organisatie opnieuw te ontwikkelen dan wel binnen te halen.

- Integriteit; Bij de aanname van medewerkers worden een aantal acties uitgevoerd om vast te stellen of de persoon integer is voor het werken met privacygevoelige gegevens:
  - Diploma/referentiecheck;
  - VOG aanvragen;
  - Ondertekenen geheimhoudingsverklaring;
  - Opdrachtgever specifieke screenings.

- Actieve beoordeling op werken in lijn met informatiebeveiligingsbeleid; In hoeverre een medewerker handelt naar het informatiebeveiligingsbeleid is onderdeel van het beoordelingsgesprek. Indien een medewerker hier niet goed op acteert, worden actief waarschuwingen gegeven die kunnen resulteren in beëindiging van de dienstbetrekking. Het zelf melden van zelf veroorzaakte beveiligingsincidenten wordt veel minder negatief beoordeeld, dan dat een andere medewerker een melding doet. Dit om te voorkomen dat er een angstcultuur ontstaat.

1.4.2 LOGISCHE EN FYSIEKE TOEGANGSBEVEILIGING

Belangrijkste maatregel is de strikt fysieke en logische scheiding van de kantoor-omgeving (zonder klantgegevens m.u.v. financiële administratie) en de productie-omgeving (met klantgegevens). Hiervoor geldt:

1 Geen enkele medewerker van Otherside heeft fysiek zelfstandig toegang tot de ruimtes waar klantgegevens zijn opgeslagen. Hiervoor is altijd medewerking van de hostingpartner (Proserve) noodzakelijk en goedkeuring van de directie;
2 Medewerkers van Proserve kunnen fysiek bij de apparatuur waar klantgegevens zijn opgeslagen. Deze gegevens zijn echter opgeslagen op geëncrypte schijven en in geëncrypte databases, waardoor voor medewerkers van Proserve de klantgegevens niet leesbaar zijn;
3 De fysieke toegang tot de kantooromgeving wordt door de facility manager vastgelegd in een sleutelplan en jaarlijks door de directie beoordeeld. De ruimtes die in dit sleutelplan worden behandeld zijn: werkplekken (algemeen), werkplek financiële administratie, serverruimte kantooromgeving (geen klantgegevens) en archief met administratie;
4 De logische toegang tot de kantooromgeving wordt door werkplekbeheer operationeel beheerd. Ook hiervoor geldt dat de uitdraai van de active directory en toegangsrechten op de verschillende servers jaarlijks wordt gecontroleerd door de directie;
5 In het indiensttredings- en uitdiensttredingsprotocol is een checklist opgenomen waarmee wordt gecontroleerd of alle fysieke en logische toegang is afgesloten. Daarnaast zijn in de checklist een aantal andere stappen opgenomen aangaande het inleveren van apparatuur en aanverwante zaken;
6 De logische toegang tot de productie-omgeving is apart afgeschermd:

a Er is voor een beperkte set medewerkers toegang tot de productie-omgeving. Dit uitsluitend indien noodzakelijk voor de uitoefening van eigen functie;
b Medewerkers met toegang krijgen een aparte gebruikersnaam en wachtwoord, geïnstalleerd certificaat en een tweede factor (time-based token) om in te loggen op de productie-omgeving. Inloggen gaat door middel van een VPN-verbinding, wat alleen mogelijk is vanaf de IP-range van kantoor Otherside dan wel een back-up-locatie;
c Toegang voor geautoriseerde medewerkers tot de servers is beperkt op basis van functie. Alleen de voor de eigen functie noodzakelijke servers zijn toegankelijk;
d Toegangsrechten worden actief bijgewerkt bij functiewijzigingen en uitdiensttreding. De verstrekte rechten worden jaarlijks door de directie gecontroleerd op juistheid;
e Toegang tot productie-databases via de webinterface zijn, net zoals voor alle andere gebruikers, altijd beveiligd met 2-factor-authenticatie;
f Webverkeer is altijd beveiligd via SSL, waarbij de SSL-instellingen via externe tools getoetst worden op bekende kwetsbaarheden. Bestandsuitwisselingen verlopen via Webservices of SFTP.

Het beheer van fysieke en logische toegang is ondergebracht in de toegangsmanagementprocedure die eveneens onderdeel is van het ISO27001:2013 gecertificeerde ISMS.

1.4.3 BEHEER, VERBINDINGEN EN INFRASTRUCTUUR

Binnen de Xpert Suite kunnen klantbeheerders zelf rollen definiëren en toekennen aan gebruikers. Op basis van deze rollen wordt door de software bepaald welke wijzigingen gebruikers wel, en welke zij niet mogen doorvoeren. Basis van deze autorisatie is dat de rol bepaalt wat een gebruiker mag doen en dat de koppeling aan medewerkersdossiers van de individuele gebruiker bepaalt voor wie dat mag. Tezamen bepalen deze autorisaties of een wijziging wel of niet wordt toegestaan. Hierbij geldt uiteraard dat alle binnenkomende wijzigingen door de server op de ingerichte autorisaties worden beoordeeld. Beheerders kunnen een IST-matrix van de wat autorisaties en alle ingerichte rollen uitdraaien om deze intern te laten toetsen (IST vs SOLL).

Otherside voert voor werkgevers het beheer van de medische dossiers in de Xpert Suite in opdracht van de ingehuurde arbodienst / bedrijfsarts uit. Het functioneel beheer omvat alle beheerwerkzaamheden t.b.v. de medische dossiers, zoals nieuwe documenten toevoegen, gebruikers toevoegen, autorisaties toevoegen of aanpassen, echter altijd in opdracht van de arbodienst / bedrijfsarts in verband met de richtsnoeren van de Algemene verordening gegevensbescherming (AVG).

Voor het beheer van de servers, waarop de software en klantgegevens staan, geldt dat een medewerker van Otherside ook een in de Active Directory gedefinieerde rol toegewezen krijgt. Deze rol-toewijzing wordt bijgehouden en periodiek gecontroleerd op juistheid. Vervolgens wordt het standaard windows-mechanisme gebruikt voor beperking van rechten. Voor toegang tot de beheeromgeving moet een VPN-verbinding worden gelegd die een IP-filtering en een 2-factor-authenticatie kent. Toegang is daarnaast uitsluitend mogelijk vanaf de IP-range van kantoor Otherside dan wel een backup-locatie.

Als aanvullende maatregel heeft Otherside een SIEM ingericht die zowel het dataverkeer als de logging van uitgevoerde acties verzamelt en analyseert. Hiermee kan aanvullend worden beoordeeld en actief worden geëscaleerd indien een gebruiker of softwarecomponent ‘ongewone’ acties verricht.

Al het verkeer naar de productie-omgeving komt via een fysieke firewall binnen, waarbij alleen verkeer wordt toegestaan wat expliciet wordt opengezet en dus is goedgekeurd via de change-procedures. Vervolgens wordt het verkeer

gerouteerd over een gesegmenteerd netwerk, waarbij alleen de web- en koppeling servers die daarvoor bedoeld zijn bereikbaar zijn via internet.

Webverkeer is altijd beveiligd via SSL, waarbij de SSL-instellingen via externe tools getoetst worden op bekende kwetsbaarheden. Bestandsuitwisselingen verlopen via VPN of SFTP.

De databaseservers zijn niet rechtstreeks te benaderen en de databases zijn per Opdrachtgever gescheiden. Opgeslagen data wordt middels het TDE-mechanisme van SQL Server geëncrypt én er vindt daarnaast cell-level encryptie plaats voor medische gegevens die door bedrijfsartsen worden ingevoerd. De cell-level encryptie vindt plaats via de applicatie met een klant- en applicatiesleutel.

1.4.4 MONITORING EN VERBETERING BEVEILIGINGSMAATREGELEN EN -INCIDENTEN

Non-conformiteiten kunnen op een aantal manieren worden vastgesteld:

1 Tijdens de jaarlijkse interne audit;

2 Tijdens de jaarlijkse externe certificeringsaudit;

3 Als gevolg van de analyse van een gemeld beveiligingsincident.

Beveiligingsincidenten kunnen worden gemeld door Opdrachtgever(s) of medewerkers of het gevolg zijn van een (periodieke) controle van een beheersmaatregel door een verantwoordelijke contactpersoon.

Na het vaststellen van een non-conformiteit wordt een plan van aanpak opgesteld. Dit plan van aanpak richt zich op de vraag welke maatregelen noodzakelijk zijn de vastgestelde non-conformiteit op te heffen en te voorkomen dat deze herhaaldelijk optreedt. Een conclusie hierin kan bijvoorbeeld zijn dat ingerichte werkwijzen dusdanig suboptimaal zijn, dat de verleiding om deze te omzeilen te groot is en aanpassingen nodig zijn.

Om te monitoren of genomen maatregelen het gewenste effect hebben, wordt bij elke maatregel expliciet vastgesteld op welke manier en hoe vaak de effectiviteit wordt gemeten. De verantwoordelijke contactpersonen voeren de vastgestelde maatregelen vervolgens uit. Tijdens de audit wordt voor alle controls gecontroleerd of dit wel is gedaan.

Beveiligingsincidenten worden in periodieke awareness-sessies en, indien door een individu dan wel afdeling veroorzaakt, met de betrokken medewerkers besproken. Indien een beveiligingsincident leidt tot een (potentieel) datalek wordt de procedure ‘Meldplicht Datalekken’ gevolgd. Binnen deze procedure dienen verantwoordelijken binnen 24 uur te worden geïnformeerd conform de richtlijnen van de Autoriteit Persoonsgegevens.

1.4.5 SOFTWAREONTWIKKELING EN INFORMATIEBEVEILIGING

Otherside heeft Secure Development principes in haar ontwikkelmethodiek opgenomen. Bij elke individuele wijziging wordt, conform de eisen in de ISO 27001 richtlijnen, beoordeeld wat de impact op het gebied van beveiliging is. Ontwikkelaars maken hierbij gebruik van een checklist die is opgesteld op basis van de OWASP-top 10 richtlijnen, ISO27002 controls, NCSC en NIST. Bij elke release wordt aan de hand van deze checklist de gewijzigde code gereviewd en opgeleverd aan de Xpert Desk. Vervolgens voert de Xpert Desk een aantal technische en functionele acceptatietests uit, waarbij de werking van autorisaties wordt getoetst voordat de release in productie wordt genomen.

Minstens éénmaal per jaar wordt een externe partij gevraagd om PEN-testen uit te voeren op de software. Hierbij wordt elke 2 jaar gewijzigd van PEN-test leverancier om een kritische analyse te waarborgen. Het betreft altijd gerenommeerde partijen zoals (maar niet beperkt tot) Deloitte, Dionach en Fox IT.

Secure programming competenties van ontwikkelaars worden met behulp van internen en externen ontwikkeld en up-to-date gehouden.

1.4.6 BACK-UP & RESTORE PROCEDURES

Otherside verplicht zich tot optimale beschikbaarheid van de Xpert Suite. Ten behoeve daarvan maakt Otherside dagelijks back-ups van de applicatie, database en logfiles op een remote-server met de beschikbaarheid van een uitwijklocatie. Tevens zullen mutaties ten aanzien van Xpert Suite continue worden vastgelegd in logfiles. Standaard wordt een historie van maximaal zeven dagen gehanteerd. Indien overeengekomen in het contract, beslaat de historie een langere periode.

Data wordt tegen vernietiging beschermd middels een back-up proces dat de afgelopen 7 dagen, 4 weken en 6 maanden wordt uitgevoerd op klantdatabases. De back-ups worden geëncrypt en periodiek getoetst door middel van restores.

Otherside heeft een permanente back-up locatie ingericht. Mocht de primaire locatie vernietigd worden, dan kan de applicatie weer up-and-running worden gebracht binnen 24 uur.

Doordat er losse back-ups per Opdrachtgever zijn, is restoren per Opdrachtgever mogelijk. Otherside kan mede hierdoor eenvoudig garanderen dat, indien dit gewenst is, alle data van een specifieke Opdrachtgever kan worden verwijderd. Gedeeltelijke verwijdering van gegevens in de back-upomgeving is niet mogelijk. De back-ups zullen automatisch binnen 6 maanden worden vernietigd.

Opdrachtgever kan een verzoek tot een Restore actie aangeven via de Xpert Desk. Indien de Restore een gevolg is van foutief of ondeskundig gebruik van Xpert Suite zullen de kosten in rekening worden gebracht. Bij calamiteiten kan Opdrachtgever ervoor kiezen met een back-up-versie van de database verder te werken. De back-up worden op een andere server geplaatst, waardoor het verlies van gegevens bij een calamiteit zo veel mogelijk wordt beperkt. De kosten op basis van de geldende tarieven (vraag vooraf naar de werkelijke tarieven) voor deze Restores zullen in rekening worden gebracht.

Het proces van deze aanvraag verloopt als volgt:

- Opdrachtgever vraagt de Restore telefonisch aan bij de Xpert Desk. Er wordt een Serviceverzoek-ticket aangemaakt;
- Deze vraag vermeldt de referentiedatum van de back-up waarop de restore moet worden geleverd;
- De Delivery Manager van Otherside bevestigt de ontvangst van de vraag, de kosten en de uitvoering overeenkomstig de vraag. Op basis van wederzijds overleg zal in deze schriftelijke bevestiging worden aangegeven wanneer de restore zal worden uitgevoerd (normaliter binnen twee werkdagen);
- De restore wordt door Opdrachtgever gecontroleerd en, indien akkoord, wordt een schriftelijke décharge door de contactpersoon van Opdrachtgever aan de Delivery Manager van Otherside opgeleverd.

1.4.7 BEWAARTERMIJNEN EN VERNIETIGING

Otherside faciliteert de Opdrachtgever in het voldoen aan de bewaartermijnen en tijdige vernietiging van data. Otherside zal nimmer zelfstandig data vernietigen, zonder dat hier een expliciete opdracht van de Opdrachtgever aan ten grondslag ligt, dan wel de beëindigingsprocedure uit de Algemene Voorwaarden is gevolgd. Gedeeltelijke verwijdering van gegevens in de back-upomgeving is niet mogelijk. Na vernietiging van gegevens op de productieomgeving zijn de gegevens in de back-ups nog slechts 6 maanden beschikbaar.

1.5 EXITPROCEDURE

Indien de overeenkomst tussen Otherside en Opdrachtgever op reguliere wijze wordt beëindigd en indien Opdrachtgever aan al haar verplichtingen heeft voldaan jegens Otherside, dan zal Otherside de gegevens eenmalig plaatsen in een back-up bestand van een MS SQL server database, terug in te lezen in de MS SQL server van Opdrachtgever. Hieraan zijn geen kosten verbonden.

Daarnaast is het mogelijk voor Opdrachtgever om een export in Excel of RTF te ontvangen. Hierbij worden de volgende gegevens in Excel-formaat aangeleverd:

- Organisatiegegevens;
- Medewerkergegevens;
- Verzuimhistorie;
- Formuliervelden (gegevens ingevoerd op schermen);
- Taken, notities, opdrachten en contactmomenten (lopend, uitgevoerd).

De documenten uit de Xpert Suite worden, gesplitst in medisch en niet-medisch, aangeleverd in RTF. De geüploade documenten worden geleverd in het formaat zoals ze zijn geüpload. De kosten (op basis van de tarieven in 2020, vraag vooraf naar de werkelijke tarieven) voor deze exports zullen in rekening worden gebracht:

- € 861 excl. BTW voor de documentenexport;
- € 574 excl. BTW voor de Excel-export.

Het proces van deze aanvraag verloopt als volgt:

- Opdrachtgever vraagt schriftelijk of per e-mail de data op bij de Opdrachtgevers Delivery Manager van Otherside. In deze aanvraag staan vermeld op welke peildatum de data moet worden opgeleverd en of er meerdere opleveringen (bijv. 1 proefaanlevering op datum X en 1 definitieve aanlevering op datum Y) of één oplevering dient te geschieden;
- De Delivery Manager van Otherside bevestigt de ontvangst van de aanvraag en de uitvoering conform de aanvraag met bijbehorende condities zoals opgenomen in dit exitplan. Tevens wordt in deze schriftelijke bevestiging, op basis van onderlinge afstemming, vastgelegd op welke wijze de data wordt aan welke geautoriseerde persoon aangeleverd (per SFTP, per beveiligde dvd etc.);
- De data wordt op de overeengekomen datum en via de vastgestelde methode aan de contactpersoon van Opdrachtgever;
- De data wordt door Opdrachtgever gecontroleerd en, indien akkoord, wordt een schriftelijke décharge door de contactpersoon van Opdrachtgever aan de Delivery Manager van Otherside opgeleverd;
- Otherside zal alle bestanden en data van Opdrachtgever maximaal 60 dagen nadat de overeenkomst is beëindigd als gevolg van opzegging of ontbinding opslaan en beschikbaar houden zodat Opdrachtgever (of de door Opdrachtgever aangewezen Derde) zijn bestanden en data kan opvragen of vernietigen. Na ommekomst van die termijn zal Otherside de bestanden en data verwijderen tenzij Opdrachtgever Otherside Schriftelijk verzoekt om de bestanden en data gedurende een alsdan nader door Opdrachtgever te bepalen aanvullende termijn te bewaren. Gedeeltelijke verwijdering van gegevens in de back-upomgeving is niet mogelijk. Na vernietiging van gegevens op de productieomgeving zijn de gegevens in de back-ups nog slechts 6 maanden beschikbaar.

1.6 OVERLEGSTRUCTUUR EN SLA RAPPORTAGE

Opdrachtgever ontvangt op verzoek van Opdrachtgever de servicerapportage van Otherside van het afgelopen kalenderkwartaal. De SLA-rapportage beschrijft minimaal:

- Een overzicht van het aantal geregistreerde tickets in het afgelopen kwartaal naar soort incident:
  - Functionele Vragen;
  - Bugs;
  - Storingen;
- Een overzicht van het aantal geregistreerde tickets in het afgelopen kwartaal naar soort wijzigingen:
  - Serviceverzoeken;
  - Productsuggesties;
- Een overzicht van het aantal gesloten tickets per soort incident met een maximale historische periode van 6 maanden;
- Een overzicht van het aantal tickets per status:
  - die in behandeling zijn bij Otherside;
  - die buiten Otherside worden geparkeerd;
- Een overzicht van de incidenten in het afgelopen kwartaal;
  - Welk % van de Bugs tijdig is opgelost en welk % niet tijdig;
  - Over welk % van de Storingen tijdig is gereageerd en over welk % niet tijdig;
  - Welk % van de Storingen tijdig is opgelost en welk % niet tijdig;
- De beschikbaarheid voor de Xpert Suite in het afgelopen kwartaal.

Indien niet voldaan wordt aan het afgesproken Service Level, dan wel indien er andere aandachtspunten in de dienstverlening zijn, geldt het volgende escalatiemodel:

ESCALATIENIVEAU	CONTACTPERSOON OPDRACHTGEVER	CONTACTPERSOON OTHERSIDE
NIVEAU 1	Functioneel applicatiebeheerder	Werknemer Xpert Desk
NIVEAU 2	Coördinator functioneel applicatiebeheer / service level manager / IT manager	Delivery Manager
NIVEAU 3	Contracteigenaar	Accountmanager
NIVEAU 4	Directie	Manager Operations

Standaard beveelt Otherside de volgende overlegstructuur aan:

2x per jaar:	Service Level Overleg (accountmanager, Delivery Manager , Opdrachtgever)
1x per kwartaal:	Business Accountoverleg (accountmanager, Opdrachtgever)
1x per jaar:	Strategisch overleg (directie en accountmanager, opdrachtgever)

In overleg met Opdrachtgever zal een definitieve overlegstructuur ingericht worden met Opdrachtgever.

2 CONTINUÏTEITS-, CAPACITEITS- & BESCHIKBAARHEIDSMANAGEMENT

2.1 HOSTING

De Xpert Suite wordt gehost in een fysiek gecertificeerd datacenter van Dataplace in Alblasserdam (www.dataplace.eu). Voor redundancy worden back-ups ook opgeslagen in een apart fysiek datacenter van EUNetworks in Amsterdam (www.eunetworks.com). Otherside garandeert een beschikbaarheid van 99,6% van de Xpert Suite en dat alle data binnen de EU/EER wordt verwerkt. De hosting bevat tevens:

- Het beschikbaar stellen van de applicatie en toegang tot de database op een internetserver;
- Beveiliging van de gegevens op de database (back-up en firewallprotectie);
- Het beheer en onderhoud van de hard- en software;
- Het beheer en onderhoud van Xpert Suite (het actueel houden van de functionaliteit met name v.w.b. wet- en regelgeving i.h.k.v. verzuim).

2.2 CONTINUÏTEIT EN ESCROW

Mocht Otherside at Work onverhoopt in een situatie komen van surseance of faillissement dan wordt de hosting van de Xpert Suite voor 6 maanden geborgd door Escrow4All. Escrow4All heeft hiervoor separate afspraken gemaakt met ProServe.

Otherside realiseert zich dat Opdrachtgever onder bepaalde omstandigheden – en uitsluitend ten behoeve van het waarborgen van de continuïteit van de Software – wenst te beschikken over de broncode van de Software. In dit verband heeft Otherside de broncode van de Software gedeponeerd bij een gespecialiseerd escrowbureau. Dit depot wordt vernieuwd op het moment dat er sprake is van belangrijke wijzigingen in de Software. In de overeenkomst met het escrowbureau is een derdenbeding ten behoeve van Opdrachtgever opgenomen, dat kortweg bepaalt dat het escrowbureau de broncode in geval van discontinuïteit van de Software onder nadere voorwaarden aan Opdrachtgever mag afgeven. Opdrachtgever kan zich als begunstigde aansluiten bij de betreffende escrowovereenkomst.

Onder voorwaarde dat de afgifte van de broncode conform de overeenkomst tussen Otherside en het escrowbureau heeft plaatsgevonden, verleent Otherside aan Opdrachtgever een gebruiksrecht strekkende tot het eigen gebruik van de Software en de aanpassing van de Software ten behoeve van onderhoud en verdere ontwikkeling. Dit voorwaardelijke gebruiksrecht houdt onder geen geval het recht in om de Software anders dan voor eigen gebruik en dat van haar eindgebruikers te exploiteren.

Opdrachtgever kan zich aanmelden als Escrow begunstigde. In de bijlage van deze SLA is een aanmeldformulier toegevoegd.

2.3 BESCHIKBAARHEID

Otherside garandeert de volgende beschikbaarheid voor de Xpert Suite:

BESCHIKBAARHEID[1]
99,6%

[1] Het betreft hier de beschikbaarheid van de gehele SaaS-oplossing Xpert Suite.

1 Otherside stelt gedurende zeven maal vierentwintig uur (7*24) per week de geleverde Xpert Suite dienst als omschreven in de Overeenkomst beschikbaar;

2 Otherside garandeert een beschikbaarheid van 99,6% met betrekking tot de geleverde SaaS-oplossing Xpert Suite als nader omschreven in de Overeenkomst. Voornoemde beschikbaarheid wordt gemeten en berekend over de periode van één (1) kalenderkwartaal. Otherside verplicht zich het door Opdrachtgever gekozen serviceniveau als beschreven in deze SLA na te komen;

3 Tot aan het Openbare Internet garandeert Otherside voor de bereikbaarheid een beschikbaarheid van 99,6% 7*24 uur op kwartaalbasis. Otherside garandeert niet dat er altijd communicatie over het Internet mogelijk is, dat er altijd een verbinding tot stand kan worden gebracht met een andere aangeslotene op het Internet of dat de dienst Xpert Suite altijd vanaf het Internet bereikbaar is. De grens is het buitenste punt op de firewall van Otherside met het openbare Internet. Als er een probleem is aan de andere kant van de grens, is het de verantwoordelijkheid van Otherside om het op te lossen;

4 De beschikbaarheidgarantie treedt in werking op het moment dat de dienst Xpert Suite werkend aan Opdrachtgever is opgeleverd;

5 Opdrachtgever dient Storingen die de dienst Xpert Suite betreffen zo spoedig mogelijk telefonisch of middels elektronische weg te melden bij de Xpert Desk;

6 De periode van “niet-beschikbaar-zijn” gaat in op het moment dat de Opdrachtgever meldt en/of Otherside constateert dat de dienst Xpert Suite niet meer functioneert conform de tussen partijen overeengekomen specificaties als vermeld in deze SLA;

7 De periode van “niet-beschikbaar-zijn” wordt afgesloten op het moment dat door Otherside aan Opdrachtgever wordt gemeld dat de dienst Xpert Suite weer functioneert conform de tussen partijen overeengekomen specificaties als vermeld in deze SLA;

8 De Beschikbaarheid (B) wordt als volgt berekend:

   a A: ((Nt - Dt)/Nt) x 100%;

   b Nt: Tijdsperiode dat de Apparatuur en/of Programmatuur beschikbaar dient te zijn;

   c Dt: Tijdsperiode dat de dienst niet beschikbaar is (tijd tijdens regulier Onderhoudsvenster niet meegerekend).

Gedurende het Onderhoudsvenster is de beschikbaarheidgarantie niet van toepassing. De beschikbaarheid wordt gemeten over de periode van één volledig kalenderkwartaal. De beschikbaarheid van de service en de toegangsbeveiliging wordt 24 uur per etmaal en 7 dagen per week gemonitord.

3 INCIDENT MANAGEMENT

Met incident management bedoelen we de behandeling van ondersteuningsvragen en het oplossen van storingen. Het doel van incident management is de normale dienstverlening zo snel mogelijk te herstellen om de gevolgen tot een minimum te beperken door de werking van een specifieke functionaliteit uit te leggen of een storing te onderzoeken en op te lossen.

3.1 TYPE INCIDENTEN

We onderkennen drie categorieën incidenten:

- Functionele Vraag (Functional Question);
- Bug (Bug);
- Storing (Malfunction).

3.2 FUNCTIONELE VRAAG (FUNCTIONAL QUESTION)

Zoals eerder besproken, voert de functioneel applicatiebeheerder van Opdrachtgever eerstelijns servicedeskactiviteiten uit voor de gebruikers van Opdrachtgever. Functionele en technische vragen over de werking van de Xpert Suite, waarvoor de functioneel applicatiebeheerder(s) en de eerstelijns ondersteuners van de Opdrachtgever geen oplossing weten of waarvoor de Opdrachtgever de oplossing niet zelfstandig kan realiseren, kunnen door de (functioneel applicatiebeheerder(s) en key users van de) Opdrachtgever onbeperkt gesteld worden bij het Tweedelijns Support onderdeel van de afdeling Xpert Desk van Otherside.

Ondersteuning is onderworpen aan een fair use policy. Indien gebrek aan ervaring van de functionele applicatiebeheerder de reden is dat er relatief veel ondersteuning wordt gegeven, zal de Delivery Manager contact opnemen met de Opdrachtgever om de te leveren dienst te bespreken en een werkomschrijving of nieuw addendum op te stellen.

3.3 BUG (BUG) EN STORING (MALFUNCTION)

Wanneer gemeld wordt dat de Xpert Suite niet functioneert op de wijze die er redelijkerwijs van verwacht mag worden (ter definitieve oordeel van Otherside) en het gemelde probleem alleen opgelost kan worden door het wijzigen van deze applicatie, spreken we van een Bug. Wanneer het gemelde probleem wordt veroorzaakt door een gebrekkige werking van het platform en daardoor alleen kan worden opgelost door de infrastructuur aan te passen, wordt dit een Storing genoemd.

3.4 PRIORITEITSTELLING INCIDENTEN

Nadat een Functionele Vraag, Bug of een Storing is goedgekeurd, zal de prioriteit worden bepaald. We onderkennen drie categorieën goedgekeurde incidenten:

- **Lage impact**: het incident heeft zeer weinig impact op het werken met Xpert Suite, er is bv. een workaround beschikbaar. Het incident leidt niet tot inconsistentie van gegevens en de integriteit, beveiliging en privacy van gegevens zijn gedekt. Werken aan een oplossing heeft een lage prioriteit;
- **Middelgrote impact**: het incident kan worden verholpen door een kleine wijziging in de applicatie of het platform. Voor het oplossen van een Bug of Storing wordt meestal geen functioneel en/of technisch ontwerp gemaakt. Wel wordt de bestaande documentatie in overeenstemming gebracht met de aanpassing in de SaaS-oplossing Xpert

Suite en wordt in de servicemanagementapplicatie een korte beschrijving gegeven van de wijze waarop de Bug of Storing is opgelost. Oplossingen met hoge prioriteit worden meestal met een tussentijdse update (hotfix) 's-nachts of in het weekend in productie genomen. Andere oplossingen zullen deel uitmaken van een reguliere release en update tijdens een Onderhoudsvenster;

- **Hoge impact:** het incident kan alleen worden opgelost door de Xpert Suite-applicatie te wijzigen. In dit geval betreft het echter dusdanig omvangrijke aanpassingen dat daarvoor wel een formeel traject doorlopen moet worden, bestaande uit de volgende stappen: requirementanalyse, opstellen functionele- en technische specificaties, bouwen, testen, in productie nemen.

Urgentie wordt geassocieerd met tijd. De tijd die nodig is om de waargenomen impact te hebben:

- **Lage urgentie:**
  - De schade van het incident neemt slechts marginaal toe met de tijd;
  - Werkzaamheden die niet door het personeel kunnen worden voltooid, zijn niet tijdgevoelig;
- **Middelhoge urgentie:**
  - De schade van het incident neemt aanzienlijk toe met de tijd;
  - Een enkele gebruiker met VIP-status is getroffen;
- **Hoge urgentie:**
  - De schade van het incident neemt snel toe met de tijd;
  - Werkzaamheden die niet door het personeel kunnen worden voltooid, zijn zeer tijdgevoelig;
  - Door onmiddellijk te handelen kan worden voorkomen dat een klein incident een groot incident wordt;
  - Meerdere gebruikers met VIP-status zijn getroffen.

Incidenten worden op basis van prioriteit afgehandeld, met gebruik van de prioriteitsmatrix:

		URGENTIE		
		Laag	**Middelhoog**	**Hoog**
IMPACT	**Laag**	Prioriteit 3	Prioriteit 3	Prioriteit 2
	Middelgroot	Prioriteit 3	Prioriteit 2	Prioriteit 1
	Hoog	Prioriteit 2	Prioriteit 1	Prioriteit 1

Hierdoor worden er drie typen prioriteit onderscheiden:

1. **Prioriteit 3**:
   i Lage impact Bugs en Storingen: Bedrijfsfuncties zijn mogelijk, echter door de gebruiker wordt de foutsituatie als hinderlijk ervaren;
   ii Alle Functionele Vragen;

2. **Prioriteit 2**:

   i Middelgrote impact Bugs en Storingen: Niet-bedrijfskritische functies zijn geblokkeerd;

3. **Prioriteit 1**:

   i Hoge impact Bugs en Storingen: Bedrijf kritische functies zijn geblokkeerd. Een workaround-oplossing kan gewenst / noodzakelijk zijn.

De prioriteit wordt door de Opdrachtgever bepaald waarna Otherside deze toetst. In geval van verschillende inzichten zal dit via de vastgestelde escalatielijnen worden opgelost.

Otherside checkt of het ticket:

- Is geplaatst in het juiste type incident (Functionele Vraag, Bug of Storing);
- De juiste prioriteit is toegekend (1, 2 of 3).

Wanneer het type incident en/of prioritering volgens Otherside onjuist is, vindt terugkoppeling naar Opdrachtgever plaats. Escalatie vindt plaats conform het escalatiemodel.

3.4.1 BIJZONDERE INCIDENTEN: SECURITY (SECURITY INCIDENT)

Daarnaast onderkent Otherside security-incidenten als bijzondere categorie. Deze worden aan de hand van een risico-analyse (hoeveel data, welke soort data, kans op misbruik) beoordeeld. Indien er grote gevolgen voor klanten, betrokkenen of Otherside zijn, worden direct maatregelen genomen om het beveiligingsincident op te lossen. Hierbij kan de keuze gemaakt worden om breder data onbereikbaar te maken voor gebruikers, zodat ook een eventueel datalek wordt gestopt. Verder gelden de procedures zoals in paragraaf 1.4 beschreven.

3.5 SERVICELEVELS INCIDENTEN

Voor de afhandeling van incidenten door de Xpert Desk gelden de volgende servicelevels. Eerstelijnsondersteuning en functioneel beheer vallen niet onder deze servicelevels.

	BESCHRIJVING	REACTIESNELHEID	OPLOSTIJD [1]
PRIORITEIT 3	Bugs en Storingen: Bedrijfsfuncties zijn mogelijk, echter door de gebruiker wordt de foutsituatie als hinderlijk ervaren Functionele Vragen	75% binnen 8 uren	75% in overeenstemming met de planning (indien er een gezamenlijk besluit is genomen) [2]
PRIORITEIT 2	Bugs en Storingen: Niet bedrijf kritische functies zijn geblokkeerd	90% binnen 4 uren	75% binnen 1 werkweek
PRIORITEIT 1	Bugs en Storingen: Bedrijf kritische functies zijn geblokkeerd. Een workaround-oplossing kan gewenst / noodzakelijk zijn. Beveiligingsincidenten	99% binnen 30 minuten [3]	75% binnen 1 werkdag

[1] Buiten kantoortijden en op feestdagen worden alleen incidenten van prioriteit 1 afgehandeld. Prioriteit 3 en 2 worden vanaf de eerstvolgende werkdag conform bovenstaande servicelevels afgehandeld.
[2] Het gaat hierbij om de planning zoals overeengekomen met Opdrachtgever en toegewezen aan een release.
[3] De reactietijd bij prioriteit 1 incidenten kan alleen worden gegarandeerd indien de melding telefonisch wordt gedaan of via prioriteitsemail (zie 1.3.1).

4 CHANGE MANAGEMENT

4.1 AARD VAN DE WIJZIGINGEN

We onderkennen twee categorieën wijzigingen:

- Serviceverzoeken (Service Request);
- Productsuggestie (Product Suggestion).

4.2 SERVICEVERZOEK (SERVICE REQUEST)

Voor ondersteuning op afstand of online-ondersteuning die niet onder de soorten incidenten valt, wordt een ticket geclassificeerd als Serviceverzoek. Dit omvat uitbesteding van of ondersteuning:

- (Her)configuratie;
- (Her)implementaties van functionaliteiten en processen;
- Import en export van gegevens;
- Herstelacties;
- Gegevenswijzigingen. het aanbrengen van correcties in de Xpert Suite-database die de eerstelijnsondersteuning van de Opdrachtgever niet zelf via de applicatie kan aanbrengen (bv. correctie van een ziektetraject);
- Trainen van gebruikers van Xpert Suite en functionele applicatiebeheerders;
- Het maken van een kopie van de database (bv. t.b.v. trainingen).

Opmerking: In verband met de AVG voert Otherside uitsluitend correcties door op de Xpert Suite database, nadat Otherside hiervoor een expliciet akkoord heeft ontvangen van de (klant van) de Opdrachtgever.

De Accountmanager of Delivery Manager zal een dergelijk verzoek in behandeling nemen en contact opnemen met de Opdrachtgever om de te leveren dienst te bespreken en een werkomschrijving op te stellen. Voor het afhandelen van Serviceverzoeken kan Otherside kosten in rekening brengen. Otherside zal vooraf aangeven wanneer er kosten worden doorbelast, gekoppeld aan het betreffende Serviceverzoek. Otherside zal pas met de uitvoering starten na akkoord van de Opdrachtgever.

4.3 PRODUCTSUGGESTIE (PRODUCT SUGGESTION)

De Xpert Suite wordt voortdurend verbeterd en uitgebreid met nieuwe functionaliteiten. Otherside luistert zorgvuldig naar haar klanten en gebruikers. Zij kunnen invloed uitoefenen op de prioriteiten van de roadmap voor de productontwikkeling door Otherside feedback te geven en ideeën te delen voor functionele wijzigingen of toevoegingen aan de Xpert Suite. Deze ideeën worden Productsuggesties genoemd.

Productsuggesties kunnen worden ingediend bij de Xpert Desk en zullen worden beoordeeld door het product management team van Otherside of deze Productsuggestie past binnen de productstrategie van Otherside en de behoeften van haar klanten. In het algemeen zullen alleen Productsuggesties van algemene aard (van belang voor meerdere Opdrachtgevers) worden aangenomen als onderdeel van de roadmap voor de productontwikkeling. In alle gevallen zullen wijzigingen aan alle klanten ter beschikking worden gesteld, tenzij uitdrukkelijk anders is overeengekomen.

Als Otherside de Productsuggestie overneemt, wordt de functionele wijziging opgenomen in de product roadmap. Wanneer de overeenkomstige functionele wijziging is gerealiseerd, zal deze worden vrijgegeven als onderdeel van een geplande release en worden opgenomen in de overeenkomstige release note. De Opdrachtgever ook afzonderlijk door de Xpert Desk op de hoogte worden gebracht.

Indien de Opdrachtgever de prioriteit van zijn Productsuggestie wenst te verhogen, kan Otherside gevraagd worden een offerte te maken voor de overeenkomstige wijziging. Otherside zal aan de Opdrachtgever een offerte voorleggen voor de realisatie van de specifieke uitbreiding, die in de Xpert Suite wordt opgenomen. Nadat de Opdrachtgever de offerte heeft geaccordeerd, zal Otherside de wijziging inplannen en realiseren. Ook voor deze wijzigingen gelden de bepalingen zoals opgenomen in deze SLA.

In veel gevallen zoekt Otherside naar co-creatie met de Opdrachtgever bij het realiseren van algemene Productsuggesties. Dit houdt in dat Otherside intensief samenwerkt met de Opdrachtgever bij het opstellen van de requirements en het realiseren van de software, maar ook dat regelmatig een financiële samenwerking wordt gezocht, die het voor beiden aantrekkelijk maakt. Deze manier van werken maakt een snellere verwezenlijking van de doelstellingen van de strategische roadmap voor de productontwikkeling van de Xpert Suite en klantgerichte productverbeteringen mogelijk.

4.4 SERVICELEVELS WIJZIGINGEN

Reactietijd naar Opdrachtgever binnen 4 weken. Oplostijd in overeenstemming met de planning (indien er een gezamenlijk besluit is genomen).

5 RELEASE MANAGEMENT

5.1 VERSIEBEHEER EN DEPLOYMENT

Voorafgaand aan de installatie van nieuwe releases, zal Otherside de release notes van de komende release overhandigen aan de bekende functionele applicatiebeheerders. Op verzoek van de Opdrachtgever installeert Otherside de nieuwe versie van Xpert Suite (Beta release) op de test/acceptatie omgeving voor de Opdrachtgever uiterlijk 5 werkdagen voor de releasedatum. Op de aangegeven releasedatum installeert Otherside de nieuwe softwareversie (release of update) op de productieomgeving. Installatie van de nieuwe releases/updates van de acceptatie- naar productieomgeving vindt plaats via een geautomatiseerde procedure (script). De Opdrachtgever heeft dan uiterlijk tot 3 werkdagen voor de releasedatum om gemotiveerd bezwaar te maken tegen het in productie nemen van een release. In dat geval zullen Opdrachtgever en Otherside in overleg treden of de release voor de Opdrachtgever, dan wel voor alle Opdrachtgever(s) wordt uitgesteld of dat de Opdrachtgever toch op de release mee gaat.

Otherside garandeert hierbij tenminste het volgende:

- Gegevensuitwisselingen met HR-systemen en/of andere aan de Xpert Suite gekoppelde systemen blijven intact v.w.b. de verwerking aan de kant van de Xpert Suite;
- Eventuele specifieke Productverbetering en de inrichting van de Xpert Suite blijven ongewijzigd werken;
- Er ontstaan geen compatibiliteitsproblemen met de reeds in de Xpert Suite ingevoerde data en gegevens;
- Standaard worden alle gegevens in de test-/acceptatieomgeving geanonimiseerd door een geautomatiseerde procedure (script);
- De Opdrachtgever kan eenmaal per kalenderkwartaal kosteloos een nieuwe test-/acceptatieomgeving aanvragen;
- Indien de Opdrachtgever de test/acceptatie omgeving gedurende 6 maanden niet heeft gebruikt, zal deze test-/acceptatieomgeving standaard worden verwijderd. Op verzoek van de Opdrachtgever zal de creatie van een nieuwe test-/acceptatieomgeving worden gepland.

5.2 ONDERHOUDSVENSTER

Voor het onderhoud van de servers en andere hardware en het plaatsen van releases kan de beschikbaarheid van Xpert Suite (productieomgeving) voor korte tijd worden onderbroken. Onderhoud wordt uitgevoerd in dal periodes (weekend) om de beschikbaarheid zo min mogelijk te frustreren. Als de service door onvoorziene omstandigheden voor langere tijd wordt onderbroken worden alle in-service partners en de functioneel applicatiebeheerders van de Opdrachtgever(s) van Otherside hiervan op de hoogte gesteld.

ACTIVITEIT	GEPLAND	TIJD (GMT +1)
Bugfixes[1]	Dagelijks (indien aan de orde)	20.00h - 21.00h
Releases en updates (Slow Track)	Op donderdag (eenmaal per 9 weken)	20.00h - 21.00h
Releases en updates (Fast Track)	Op woensdag (eenmaal per 2 weken)	20.00h - 21.00h

[1] Spoedeisende werkzaamheden kunnen bij uitzondering ook tijdens kantoortijden worden uitgevoerd. Otherside stelt Opdrachtgever hiervan op een zo vroeg mogelijk moment schriftelijk dan wel telefonisch op de hoogte.

ACTIVITEIT	GEPLAND	TIJD (GMT +1)
Releases en updates	Op zaterdag (één keer per maand)	Zaterdag 20.00u - Zondag 02.00u
Periodieke updates van de infrastructuur	In het weekend (maximaal vier keer per jaar)	Vrijdag 20.00u - Maandag 04.00u

5.3 STRATEGISCHE RELEASEONTWIKKELING & FUNCTIONEEL ONDERHOUD

Otherside volgt haar eigen strategische productontwikkelingsagenda. Op basis van de strategische dialoog met haar Opdrachtgevers, de waargenomen marktontwikkelingen en de nieuwe technologische mogelijkheden wordt de strategische routekaart voor productontwikkeling opgesteld en voortdurend bijgewerkt. De Opdrachtgever kan lid worden van het 'UserGroup' gebruikersplatform. Via dit platform worden aanpassingen en innovaties in de Xpert Suite getoetst op onder meer haalbaarheid en functionaliteit. De sessies zijn informatief, toetsend en uiteraard interactief. UserGroup sessies zijn exclusief voor de Opdrachtgevers van Otherside en zijn kosteloos bij te wonen.

Functioneel onderhoud behelst het aanbrengen van een functionele wijziging of aanvulling in de Xpert Suite en vindt plaats op initiatief van Otherside of op verzoek van de Opdrachtgever. Op initiatief van Otherside worden de noodzakelijke functionele wijzigingen om nieuwe, of wijzigingen in, relevante wet- en regelgeving te faciliteren (bijv. naleving van de Wet verbetering poortwachter) opgenomen in de roadmap voor productontwikkeling.

6 BOETES

6.1 BESCHIKBAARHEID

Indien de Dienstverlening niet de Beschikbaarheid haalt conform artikel 2.3 van deze SLA zal Opdrachtgever gerechtigd zijn een boete van 10% van de abonnementskosten te vorderen per betreffende kalendermaand waarin de Beschikbaarheid niet is gehaald, tot een maximum van € 1.000,00 per maand.

A BIJLAGE AANMELDINGSFORMULIER ESCROW BEGUNSTIGDE

ESCROW4ALL INFORMATIE	
LEVERANCIER	Otherside at Work B.V.
SALES CONSULTANT	Timo van Ling
CONTACTGEGEVENS	Timo.vanLing@escrow4all.com

Wil als begunstigde deelnemen aan (*aankruisen wat van toepassing is*):

☐	Software Escrow (source code) als overeengekomen tussen Otherside at Work B.V. en Escrow4all B.V. (overeenkomst SW2P19694)
☐	SaaS Escrow (6 maanden hosting) als overeengekomen tussen Otherside at Work B.V. en Escrow4all B.V. (overeenkomst SA2P21805, download via link)

Benodigde gegevens ten behoeve aanmelding Escrow Begunstigde onder een Escrow4all Mantel Overeenkomst:

Gegevens Begunstigde

BEDRIJFSNAAM	
AFDELING	
BEZOEKADRES	
POSTCODE	
LOCATIE	
TELEFOONNUMMER	
POSTADRES	
POSTCODE	
LOCATIE	
LAND	

Contactpersoon

NAAM	
FUNCTIE	
TELEFOONNUMMER	
E-MAIL	

2de contactpersoon (optioneel)

NAAM	
FUNCTIE	
TELEFOONNUMMER	
E-MAIL	

Specifieke informatie

START DEELNAME	Per direct
PRODUCT	Xpert Suite
VERSIE	Laatste versie
OPMERKINGEN	

Svp volledig invullen en e-mailen naar: sales@escrow4all.com

De aanmelding wordt – na toetsing – binnen 5 werkdagen verwerkt.