VERWERKERSOVEREENKOMST MEDISCHE GEBRUIKERS

OTHERSIDE AT WORK

KENMERK	C26XXXX
VERSIE	7.1
STATUS	Definitief
DATUM	30 april 2026
CLASSIFICATIE	Gevoelig

Tussen

NAAM WERKGEVER,

NAAM ARBODIENST/ARTS GEMACHTIGDE

en

Otherside at Work

VOORBLAD BEHOREND BIJ VERWERKERSOVEREENKOMST MET NUMMER C26XXXX

Hierbij ontvangt u zoals besproken de verwerkersovereenkomst, evenals dit begeleidend voorblad waarin instructies opgenomen zijn ten behoeve van het correct invullen van de stukken en hoe deze te retourneren. De overeenkomst dient volledig ingevuld en ondertekend te worden. Tevens dient elke pagina voorzien te zijn van een paraaf. De tenaamstellingen van Opdrachtgever en de naam van de rechtsgeldige vertegenwoordiger behoren overeenkomstig het Handelsregister van de Kamer van Koophandel te zijn.

1. De ondertekende en geparafeerde Overeenkomst en bijlage(n), alsmede dit voorblad, dient u digitaal te verzenden naar customersuccess@othersideatwork.nl & uw Customer Success Manager van Otherside at Work
2. Na ontvangst per post van beide getekende exemplaren, krijgt u één door Otherside getekend exemplaar retour gestuurd. Ten behoeve van een juiste adressering dienen onderstaande gegevens ingevuld te worden.

*Firmanaam:	
*T.a.v.:	
*Postadres:	

3. Voor eventuele vragen kunt u uiteraard contact opnemen met uw contactpersoon. We danken u hartelijk voor uw medewerking.

Paraaf Opdrachtgever: *Paraaf Verwerkingsverantwoordelijke:* *Paraaf Otherside at Work:*

Ondergetekenden:

1. NAAM WERKGEVER, gevestigd en kantoorhoudende te PLAATS ([postcode]) aan [adres], hierbij rechtsgeldig vertegenwoordigd door [vertegenwoordiger], hierna te noemen "**Opdrachtgever**";

2. De [arbodienst] [naam], gevestigd en kantoorhoudende te [plaats] ([postcode]) aan [adres], hierbij rechtsgeldig vertegenwoordigd door [vertegenwoordiger], hierna te noemen "**Verwerkingsverantwoordelijke**";

3. Otherside at Work B.V., statutair gevestigd en kantoorhoudende te 's-Hertogenbosch aan Wisent 14 (5236 PX), hierbij rechtsgeldig vertegenwoordigd door de heer R.A.A. van der Sanden en de heer D.P.J. Benders, hierna te noemen: "**Verwerker**"; en

Hierna gezamenlijk te noemen: **Partijen** en elk afzonderlijk: **Partij**

Overwegende dat:

a) Opdrachtgever met Verwerker een overeenkomst is aangegaan met betrekking tot de levering van en beheer en onderhoud op de Xpert Suite (hierna: de "Overeenkomst Dienstverlening");
b) Verwerkingsverantwoordelijke in opdracht van Opdrachtgever als arbodienst en/of medische gebruiker optreedt ten behoeve van Opdrachtgever en hiervoor een dienstverleningsovereenkomst heeft gesloten met Opdrachtgever (hierna: de "Overeenkomst Bedrijfsartsen"). Waarbij Verwerkingsverantwoordelijke in de door Opdrachtgever aangekochte Software medische gegevens verwerkt;
c) Verwerker als verwerker van Persoonsgegevens voor zowel Opdrachtgever en Verwerkingsverantwoordelijke optreedt in de zin van de Toepasselijke Privacy Wetgeving;
d) Verwerkingsverantwoordelijke als verwerkingsverantwoordelijke in de zin van de Toepasselijke Privacy Wetgeving fungeert ten aanzien van de medische gegevens en mogelijk als Verwerker ten aanzien van de Persoonsgegevens niet zijnde medische gegevens;
e) Partijen dientengevolge in een driepartijenverhouding tot elkaar staan en in deze een Verwerkersovereenkomst als bedoeld in artikel 28, derde lid, van de AVG aangaan.

Komen het volgende overeen:

1 DEFINITIES

1.1 In deze overeenkomst hebben de volgende (onderstreepte) begrippen de daaropvolgende betekenis:

a.) Aanvullende Nationale Wetgeving: elke wetgeving met betrekking tot de verwerking van persoonsgegevens in een lidstaat van de EU naast de AVG.
b.) Diensten: de diensten die door Verwerker voor Verwerkingsverantwoordelijke worden verricht op basis van een Dienstverleningsovereenkomst.
c.) Dienstverleningsovereenkomst: overeenkomst tussen Opdrachtgever en Verwerker die betrekking heeft op het verrichten van Diensten.
d.) Overeenkomst Bedrijfsartsen: overeenkomst tussen Verwerkingsverantwoordelijke en Opdrachtgever die betrekking heeft op het verrichten van Diensten.
e.) Implementatiewetgeving: de toepasselijke nationale wetgeving die in het betreffende land van toepassing is op de verwerking van persoonsgegevens in het kader van de Diensten, waaronder de wetgeving die is

Paraaf Opdrachtgever: Paraaf Verwerkingsverantwoordelijke: Paraaf Otherside at Work:

geïmplementeerd om uitvoering te geven aan de Privacyrichtlijn.

f.) AVG: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

g.) Inbreuk: de Inbreuk In Verband Met Persoonsgegevens zoals gedefinieerd in de Privacy verordening.

h.) Sub-Verwerker: iedere derde partij die door Verwerker is betrokken bij de verwerking van persoonsgegevens in het kader van de Diensten.

i.) Toepasselijke Privacy Wetgeving: de Privacy verordening en de Aanvullende Nationale Wetgeving van de betreffende landen en de geldende WGBO en de Wet BIG en de richtlijnen van NVAB en de KNMG.

1.2 Elk begrip dat hier niet is gedefinieerd, maar dat wel is gedefinieerd in de Toepasselijke Privacy Wetgeving (zoals "*persoonsgegeven*", "*verwerken*", etc.), heeft in deze overeenkomst dezelfde betekenis als in de Toepasselijke Privacy Wetgeving.

1.3 Voor wat betreft de begrippen wordt in deze overeenkomst de terminologie van de Privacy verordening gebruikt (*bijv. "verwerker" i.p.v. "bewerker"*). Daarmee wordt niet bedoeld af te wijken van de betekenis van de Toepasselijke Privacy Wetgeving.

2 ALGEMEEN

2.1 Deze verwerkersovereenkomst is een bijlage bij de in artikel 1.1 vermelde Dienstverleningsovereenkomst(en).

2.2 Deze verwerkersovereenkomst heeft betrekking op de verwerking van persoonsgegevens die uit de Diensten voortvloeit, ongeacht of de betreffende Dienstverleningsovereenkomst wel of niet expliciet refereert aan de verwerking van persoonsgegevens.

2.3 De aard en de doeleinden van de verwerking, evenals het soort persoonsgegevens en de categorieën van betrokkenen die door Verwerker namens Verwerkingsverantwoordelijke worden verwerkt, staan nader uitgewerkt in Bijlage 1, bij gebreke waarvan de verwerking is beperkt tot de werkzaamheden die strikt noodzakelijk zijn voor de uitvoering van de Dienstverleningsovereenkomst.

3 HOEDANIGHEDEN EN TAKEN VAN PARTIJEN

3.1 Verwerker zal alleen op basis van schriftelijke instructies van Verwerkingsverantwoordelijke de persoonsgegevens verwerken.

3.2 Verwerkingsverantwoordelijke wordt geacht de instructies aan Verwerker te hebben gegeven voor elke verwerking die strikt noodzakelijk is in het kader van het verlenen van de Diensten. Onder deze instructies zijn mede begrepen wijzigingen aan de Diensten, voor zover de Dienstverleningsovereenkomst zulke wijzigingen toestaat.

3.3 De Verwerkingsverantwoordelijke garandeert de rechtmatigheid van het gebruik, de verwerking, de archivering, het doel van het gebruik en de uitwisseling van de Persoonsgegevens en/of ieder ander gebruik, zoals die voortvloeien uit de tenuitvoerlegging van deze overeenkomst.

3.4 In afwijking van bepaling 3.2 is het Verwerker toegestaan om de persoonsgegevens te verwerken als een wettelijk voorschrift hem tot verwerking verplicht. In dat geval stelt de Verwerker, voorafgaand aan de verwerking, Verwerkingsverantwoordelijke in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

3.5 De maximale categorieën van persoonsgegevens die partijen verwachten te verwerken en de andere gegevens die Gebruikers wensen in te voeren in de software, zijn vastgelegd in Bijlage 1.

4 GEHEIMHOUDING

4.1 Verwerker zal de persoonsgegevens tegenover derden geheimhouden en zal deze niet openbaar maken, anders dan voor zover noodzakelijk voor het verlenen van de Diensten dan wel voor zover een wettelijk voorschrift of rechterlijk bevel Verwerker tot mededeling c.q. verstrekking verplicht.

4.2 Verwerker staat er voor in en garandeert dat werknemers en alle overige natuurlijke personen die handelen onder zijn gezag en toegang hebben tot de persoonsgegevens eveneens onder dezelfde voorwaarden geheimhouding zullen betrachten ten aanzien van voornoemde informatie.

5 BEVEILIGINGSMAATREGELEN EN PERIODIEKE REVIEW DAARVAN

5.1 Verwerker zal technische- en organisatorische maatregelen nemen om de persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, alsmede om een passende mate van betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) te waarborgen. Deze maatregelen zullen passend zijn, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen.

5.2 Bij de beoordeling van een passend veiligheidsniveau zal Verwerker in het bijzonder aandacht schenken aan risico's die zich voordoen bij persoonsgegevensverwerking, zoals in het bijzonder de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

5.3 Verwerker zal in het kader van de in de vorige twee leden beschreven verplichtingen, tenminste de in Bijlage 2 gespecificeerde maatregelen treffen.

5.4 De door Verwerker in het kader van lid 1 en lid 2 te nemen maatregelen zullen in ieder geval voldoen aan de ISO27001 standaard. Verwerker zal op eerste verzoek van Verwerkingsverantwoordelijke een door een onafhankelijke en ter zake deskundige derde afgegeven certificaat overleggen ten bewijze hiervan. Het betreffende certificaat mag niet ouder zijn dan 12 maanden.

5.5 Verwerker zal periodiek de technische- en organisatorische maatregelen die genomen zijn om de verwerking te beveiligen testen, beoordelen en evalueren, al dan niet door inschakeling van een ter zake deskundige derde. Als uit deze beoordeling volgt dat de genomen maatregelen niet langer voldoende zijn, dan zal Verwerker alle redelijke stappen nemen om het beveiligingsniveau te verbeteren.

5.6 Verwerker zal al het noodzakelijke doen om te verzekeren dat enige natuurlijk persoon, die handelt onder het gezag van Verwerker en die toegang heeft tot persoonsgegevens deze gegevens niet zal verwerken tenzij op basis van instructies van Verwerkingsverantwoordelijke, of indien hij of zij daartoe verplicht wordt op grond van wetgeving.

5.7 Verwerker verleent Verwerkingsverantwoordelijke, tegen redelijke kosten, bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 t/m 36 van de Privacy Verordening.

6 INBREUK

6.1 Verwerker informeert Verwerkingsverantwoordelijke over iedere Inbreuk. Deze informatie wordt gegeven zonder onredelijke vertraging, doch in ieder geval binnen 24 uur, zodra hij daarvan kennis heeft genomen. In Bijlage 3

dienen aanspreekpunten en contactgegevens te worden vastgelegd.

6.2 In de, in het vorige lid bedoelde kennisgeving wordt ten minste het volgende omschreven of meegedeeld, voor zover Verwerker deze informatie heeft:

a.) De aard van de Inbreuk, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

b.) De naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;

c.) De waarschijnlijke gevolgen van de Inbreuk;

d.) De maatregelen die Verwerker heeft voorgesteld of genomen om de Inbreuk aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan;

e.) Enige andere informatie die Verwerkingsverantwoordelijke nodig heeft op basis van de Toepasselijke Privacy Wetgeving.

6.3 Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

6.4 Verwerker zal Verwerkingsverantwoordelijke ondersteunen bij het naleven van alle verplichtingen op basis van de Toepasselijke Privacy Wetgeving, rekening houdende met de aard van de verwerking en de informatie die beschikbaar is voor de verwerker. Deze ondersteuning houdt ook in het informeren van betrokkenen van een Inbreuk indien de Toepasselijke Privacy Wetgeving daartoe verplicht.

6.5 Verwerker documenteert alle Inbreuken, met inbegrip van de feiten omtrent de Inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen, alsmede alle andere relevante informatie omtrent de Inbreuk.

7 LOCATIE VAN GEGEVENS

7.1 Verwerker zal persoonsgegevens louter binnen de grenzen van de Europese Economische Ruimte (EER) verwerken (of doen verwerken), tenzij

a.) Het overdragen van persoonsgegeven naar buiten de EER door Verwerkingsverantwoordelijke wordt geautoriseerd of geïnstrueerd; of

b.) Wetgeving waar Verwerker aan is onderworpen, Verwerker verplicht tot overdracht naar buiten de EER. Indien Verwerker hiertoe verplicht wordt, zal Verwerker Verwerkingsverantwoordelijke terstond informeren, tenzij deze wetgeving Verwerker dit verbiedt.

8 SUB-VERWERKER

8.1 Verwerker zal geen Sub-Verwerker aanstellen, tenzij ze daartoe expliciet geautoriseerd wordt door Verwerkingsverantwoordelijke.

8.2 Verwerkingsverantwoordelijke autoriseert Verwerker hierbij om Proserve BV (Oostmaaslaan 71, 3063 AN Rotterdam) te betrekken als Sub-Verwerker.

8.3 Indien er een Sub-Verwerker wordt aangesteld, dan:

a.) Blijft Verwerker onverkort aansprakelijk voor de nakoming van de verplichtingen uit onderhavige overeenkomst;

b.) Zal Verwerker de aanstelling van een Sub-Verwerker in een schriftelijke overeenkomst vastleggen;

c.) Staat Verwerker er voor in dat alle verplichtingen die op grond van deze verwerkersovereenkomst rusten op Verwerker mede komen te rusten op deze Sub-Verwerker;

d.) Staat Verwerker er voor in dat de betreffende Sub-Verwerker ook de schriftelijke instructies van Verwerkingsverantwoordelijke opvolgt.

9 RECHTEN VAN BETROKKENEN

9.1 De Toepasselijke Privacy Wetgeving geeft de betrokkene bepaalde rechten. De verantwoordelijkheid voor het omgaan met (de uitvoering van) deze rechten rust bij Verwerkingsverantwoordelijke.

9.2 Verwerker zal, indien Verwerkingsverantwoordelijke daar om verzoekt, aan Verwerkingsverantwoordelijke alle noodzakelijke medewerking verlenen bij de nakoming van de verplichtingen van Verwerkingsverantwoordelijke verplichtingen op grond van de rechten genoemd in het vorige lid.

10 INFORMATIE, SAMENWERKING, CONTROLE EN NALEVING

10.1 Verwerker zal aan Verwerkingsverantwoordelijke alle informatie verstrekken met betrekking tot enige gedragscode of goedgekeurd certificeringsmechanisme waar zij aan gebonden is, zoals bedoeld in respectievelijk artikel 40 en artikel 42 van de Privacy verordening.

10.2 Op het eerste daartoe strekkende verzoek zal Verwerker aan Verwerkingsverantwoordelijke alle relevante informatie verstrekken betreffende de aspecten van de door hem verrichte verwerking van persoonsgegevens zodat Verwerkingsverantwoordelijke, mede aan de hand van die informatie, aan kan tonen dat zij de Toepasselijke Privacy Wetgeving naleeft.

10.3 Verwerkingsverantwoordelijke is gerechtigd om, middels een betrouwbare derde (gebonden aan geheimhouding), te controleren in hoeverre Verwerker de verplichtingen uit deze verwerkersovereenkomst naleeft. Verwerker zal aan een dergelijke controle kosteloos haar volledige medewerking verlenen.

10.4 De leden 2 en 3 zijn niet van toepassing voor zover een dergelijk verzoek of instructie:

a) Een disproportionele last voor Verwerker met zich mee brengt;

b) Niet is gerelateerd aan de verwerking van persoonsgegevens;

c) Zou leiden tot het openbaren van bedrijfsgeheimen van Verwerker;

d) Voor Verwerkingsverantwoordelijke niet zou leiden tot extra informatie bovenop de informatie die haar al is verstrekt in het kader van lid 1;

e) In strijd zou zijn met wetgeving.

10.5 Indien een van de uitzonderingen uit het vorige lid zich voordoet zal Verwerker daar Verwerkingsverantwoordelijke onmiddellijk over informeren.

11 KOSTEN

11.1 De kosten voor de verwerking van gegevens die inherent zijn aan de normale uitvoering van de Diensten, worden geacht besloten te liggen in de Dienstverleningsovereenkomst(en) gespecificeerde (reeds verschuldigde) vergoeding(en) voor de Diensten.

11.2 Enige ondersteuning of enige andere aanvullende dienstverlening die Verwerker op grond van deze verwerkersovereenkomst dient te verlenen (bijv. op grond van artikel 6.4), of die wordt verzocht door Verwerkingsverantwoordelijke, inclusief alle verzoeken tot aanvullende informatie, zullen in rekening worden gebracht bij Verwerkingsverantwoordelijke overeenkomstig de in de Dienstverleningsovereenkomst(en) gespecificeerde tarieven. Voor betreffende werkzaamheden gelden de tarieven "Technische consultancy" zoals overeengekomen in de Dienstverleningsovereenkomst tussen Verwerkingsverantwoordelijke en Verwerker.

11.3 De voorgaande bepaling is niet van toepassing indien de werkzaamheden verband houden met een tekortkoming van Verwerker onder deze overeenkomst. De werkzaamheden zullen in dat geval kosteloos worden verricht (onverminderd het recht van Verwerkingsverantwoordelijke de daadwerkelijk geleden schade op Verwerker te verhalen). De bewijslast dat de betreffende tekortkoming niet toerekenbaar is ligt bij Verwerker.

11.4 Indien Verwerker na einde van de Dienstenovereenkomst en/of Bedrijfsartsenovereenkomst op verzoek van de Verwerkingsverantwoordelijke personeelsdata dient te blijven bewaren, zullen hiervoor kosten worden gerekend.

12 AANSPRAKELIJKHEID

12.1 De aansprakelijkheid op deze verwerkersovereenkomst is overeengekomen in de Overeenkomst dan wel Algemene Voorwaarden Otherside.

12.2 Indien en voor zover in de Dienstverleningsovereenkomst de aansprakelijkheid voor onrechtmatige verwerking van persoonsgegevens geheel is uitgesloten, is deze beperking – in afwijking van het vorige lid – niet van toepassing.

12.3 Indien er als gevolg van een toerekenbare tekortkoming van Verwerker, of een aan Verwerker toerekenbaar gedragen of nalaten, aan Verwerkingsverantwoordelijke een boete wordt opgelegd door de toezichthouder of Verwerkingsverantwoordelijke wordt veroordeeld tot betalen van een schadevergoeding aan betrokkene(n) op grond van artikel 82 AVG, welke (deels) rechtstreeks verband houdt met voornoemde tekortkoming, gedragen of nalaten, dan is Verwerker aansprakelijk voor (dat deel van) die boete of schadevergoeding.

12.4 Iedere beperking van aansprakelijkheid komt voorts te vervallen in geval van opzet of grove schuld aan de zijde van Verwerker.

13 GEVOLGEN VAN DE TOEPASSELIJKE PRIVACY WETGEVING

13.1 Verwerker garandeert dat de Diensten gebruikt kunnen worden in overeenstemming met de Toepasselijke Privacy Wetgeving. Deze garantie geldt alleen voor de Toepasselijke Privacy Wetgeving in de landen die zijn beschreven in Bijlage 1, bij gebreke waarvan het land van vestiging van Verwerkingsverantwoordelijke gelezen wordt. Verwerker heeft geen kennis van andere Aanvullende Nationale Wetgeving of Implementatiewetgeving.

13.2 Verwerkingsverantwoordelijke moet Verwerker informeren over enige Aanvullende Nationale Wetgeving of Implementatiewetgeving, voor zover van belang voor de uitvoering van de Diensten, indien Verwerkingsverantwoordelijke wil dat Verwerker ook persoonsgegevens verwerkt met betrekking tot de activiteiten van Verwerkingsverantwoordelijke in andere landen van de EU, niet zijnde de landen vermeld in Bijlage 1.

13.3 Verwerker zal Verwerkingsverantwoordelijke informeren indien zij, op basis van de informatie door Verwerkingsverantwoordelijke verstrekt in overeenstemming met het vorige lid, vermoedt dat het uitvoeren van de Diensten (gedeeltelijk) in strijd is met enige Aanvullende Nationale Wetgeving of Implementatiewetgeving.

14 DUUR, BEËINDIGING EN GEVOLGEN VAN BEËINDIGING

Paraaf Opdrachtgever: *Paraaf Verwerkingsverantwoordelijke:* *Paraaf Otherside at Work:*

14.1 De duur van deze verwerkersovereenkomst is gelijk aan de duur van de Dienstverleningsovereenkomst(en) en Bedrijfsartsenovereenkomst.

14.2 Deze verwerkersovereenkomst wordt automatisch beëindigd indien alle Dienstverleningsovereenkomsten en/of Bedrijfsartsenovereenkomst zijn beëindigd.

14.3 Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging of ontbinding van de verwerkersovereenkomst voort te duren, blijven na beëindiging c.q. ontbinding van deze verwerkersovereenkomst bestaan. Tot deze verplichtingen behoren onder meer:

a.) Vrijwaring voor boetes van toezichthouders;
b.) Geheimhouding;
c.) Geschillenbeslechting, toepasselijk recht.

14.4 In het geval dat een Dienstverleningsovereenkomst of Bedrijfsartsenovereenkomst is beëindigd zal Verwerker, ter vrije keuze van Verwerkingsverantwoordelijke, de in het kader van de Diensten verwerkte persoonsgegevens vernietigen of terug leveren.

14.5 Verwerker zal na kennisname van het eindigen van de Dienstenovereenkomst, of wanneer Verwerker in kennis wordt gesteld dat Bedrijfsartsenovereenkomst eindigt, alle noodzakelijke medewerking verlenen aan de soepele overstap, bestaande uit het ter beschikking stellen van alle bestanden en data van Verwerker aan Verwerkingsverantwoordelijke. Verwerker zal alle bestanden en data van Verwerkingsverantwoordelijke maximaal 60 dagen nadat de Dienstenovereenkomst en/of Bedrijfsartsenovereenkomst is beëindigd als gevolg van opzegging of ontbinding opslaan en beschikbaar houden zodat Verwerkingsverantwoordelijke zijn bestanden en data kan opvragen of vernietigen. Na ommekomst van die termijn zal Verwerker de bestanden en data verwijderen tenzij Verwerkingsverantwoordelijke Verwerker schriftelijk verzoekt om de bestanden en data gedurende een alsdan nader door Verwerkingsverantwoordelijke te bepalen aanvullende termijn te bewaren. Na afloop van voornoemde aanvullende termijn zal Verwerker de bestanden en data alsnog verwijderen. Het bewaren van de bestanden en data gedurende de aanvullende bewaartermijn is onder uitsluitende verantwoordelijkheid van Verwerkingsverantwoordelijke.

14.6 Het terug leveren van de persoonsgegevens geschiedt in een algemeen leesbaar en deugdelijk gedocumenteerd bestandsformaat.

14.7 Ongeacht het voorgaande:

a.) Is Verwerker gerechtigd om de gegevens te bewaren indien wetgeving haar daartoe verplicht.
b.) Zal Verwerker informatie met betrekking tot Inbreuken, zoals bedoeld in artikel 6.5, tenminste tot een jaar na beëindiging van de Dienstverleningsovereenkomst(en) bewaren.

15 TOEGANG VERWERKINGSVERANTWOORDELIJKE XPERT SUITE

15.1 De door Verwerkingsverantwoordelijke in te zetten medische gebruikers verkrijgen toegang tot het deel van Xpert Suite waar de medische gegevens (kunnen) worden opgeslagen. Toegang aan de medische gebruikers wordt uitsluitend verleend met volledige inachtneming van door Verwerker voorgeschreven verificatieprocedures en protocollen. Verwerkingsverantwoordelijke is jegens Verwerker verantwoordelijk voor het juiste gebruik van Xpert Suite en voor het volgen van de protocollen ter zake. Verwerker zal Verwerkingsverantwoordelijke volledig in kennis stellen van deze toepasselijke protocollen.

15.2 Verwerkingsverantwoordelijke is geen vergoeding aan Verwerker verschuldigd voor de toegang en het gebruik van Xpert Suite van Verwerker.

15.3 Verwerker verstrekt rechtstreeks aan de door Verwerkingsverantwoordelijke ingezette medische gebruikers de

inloggegevens voor het verkrijgen van toegang tot Xpert Suite. Het gedeelte van Xpert Suite waar medische gegevens worden ingevoerd en opgeslagen is, afgezien van de systeembeheerder van Verwerker, uitsluitend toegankelijk voor degene die is geautoriseerd als medische gebruiker van Verwerkingsverantwoordelijke. De systeembeheerder van Verwerker heeft een geheimhoudingsplicht en deze is slechts technisch toegangsbevoegd. De systeembeheerder heeft geen toestemming van Verwerkingsverantwoordelijke en/of Betrokkenen voor toegang tot de inhoudelijke gegevens. Een kopie van de geheimhoudingsverklaring van de systeembeheerder is door Verwerkingsverantwoordelijke op te vragen bij Verwerker.

15.4 Verwerker is slechts gerechtigd de toegang tot Xpert Suite te blokkeren ingeval van niet-geautoriseerd gebruik dan wel misbruik. Indien Verwerker, zoals achteraf blijkt, de toegang tot Xpert Suite onterecht heeft geblokkeerd, is Verwerker jegens Verwerkingsverantwoordelijke aansprakelijk voor enige schade die Verwerkingsverantwoordelijke of een door hem ingezette medische gebruiker ter zake heeft geleden.

15.5 Op verzoek van Verwerkingsverantwoordelijke zal Verwerker alle in de Software opgeslagen medische gegevens aan Verwerkingsverantwoordelijke ter beschikking stellen in een door Verwerkingsverantwoordelijke vast te stellen format/medium/ bestand c.q. Verwerkingsverantwoordelijke daar toegang toe geven.

15.6 Verwerker zal haar volledige medewerking verlenen aan Verwerkingsverantwoordelijke om:

a.) na goedkeuring van en in opdracht van Verwerkingsverantwoordelijke en Betrokkenen, die Betrokkenen toegang te laten krijgen tot hun medische gegevens;

b.) vast te leggen en aan te tonen dat medische gegevens verwijderd of gecorrigeerd zijn indien zij verwijderd dienen te worden, dan wel indien zij incorrect zijn of, ingeval Verwerkingsverantwoordelijke het er niet mee eens is dat medische gegevens incorrect zijn, het feit vast te leggen dat de Betrokkene zijn medische gegevens als incorrect beschouwt. Bij niet aanpassen van de medische gegevens in een dergelijk geval zal de visie van de Betrokkene aan het dossier worden toegevoegd.

15.7 Verwerkingsverantwoordelijke en Verwerker vrijwaren Opdrachtgever voor iedere financiële dan wel juridische aanspraak op grond van dit artikel.

15.8 Indien door Verwerker aan Verwerkingsverantwoordelijke de toegang tot de Software wordt ontzegd ten gevolge van een geschil tussen Opdrachtgever en Verwerker, is Verwerkingsverantwoordelijke noch jegens Opdrachtgever noch jegens Verwerker aansprakelijk voor de daaruit voortvloeiende schade. Verwerkingsverantwoordelijke wordt door Verwerker 24 uur voorafgaand aan het blokkeren van de toegang door Verwerker op de hoogte gesteld van het feit dat Verwerkingsverantwoordelijke de toegang op grond van deze bepaling zal worden ontzegd.

16 OVERIGE BEPALINGEN

16.1 Voor zover enige bepaling van deze verwerkersovereenkomst in strijd is met hetgeen in de Dienstverleningsovereenkomst(en) is bepaald, prevaleert hetgeen in deze verwerkersovereenkomst is bepaald (voor zover de strijdigheid betrekking heeft op het verwerken van persoonsgegevens).

16.2 Voor alle onderwerpen die niet in deze verwerkersovereenkomst zijn geregeld geldt dat de bepalingen van de relevante Dienstverleningsovereenkomst *mutatis mutandis* van toepassing zijn op de verwerking van persoonsgegevens in het kader van die specifieke Dienst.

16.3 Wijzigingen op deze verwerkersovereenkomst en/of de bijlagen zijn alleen geldig voor zover deze schriftelijk zijn vastgelegd en zijn ondertekend door beide partijen.

16.4 Deze verwerkersovereenkomst kan (gedeeltelijk) worden vervangen door standaard contractsbepalingen als bedoeld in artikel 28 lid 6 van de Privacy verordening, indien zulke bepalingen voor beide partijen wederzijds

acceptabel zijn.

17 TOEPASSELIJK RECHT EN BEVOEGDE RECHTER

17.1 Op deze overeenkomst is Nederlands recht van toepassing. Behoudens voor zover de overeenkomst(en) met betrekking tot de Diensten een exclusief bevoegde rechter aanwijzen, is de rechter gevestigd in het arrondissement waar Verwerkingsverantwoordelijke vestigingsplaats heeft exclusief bevoegd.

Aldus overeengekomen en in tweevoud ondertekend op:

NAAM WERKGEVER	Verwerkingsverantwoordelijke :
Naam:	Naam:
Functie:	Functie:
Otherside at Work:	
R.A.A. van der Sanden	D.P.J. Benders
Chief Product Officer	CEO

Graag bijlage 3 digitaal dan wel schriftelijk de Functionaris Gegevensbescherming en/of de Information Security Officer verder aan te vullen door OPDRACHTGEVER en VERWERKERSVERANTWOORDELIJKE.

BIJLAGE 1 BIJ VERWERKERSOVEREENKOMST MEDISCHE GEBRUIKERS

SOORTEN PERSOONSGEGEVENS & CATEGORIEËN VAN BETROKKENEN

Persoonsgegevens die zullen worden verwerkt in het kader van de Overeenkomst van Opdracht:

- Van medewerkers:
    - Algemene gegevens:
        - BSN, NAW, dienstverbandgegevens (functies, afdelingen, omvang contract, etc.), contactgegevens (tel, email).
    - Gezondheidsgegevens:
        - Aan- en afwezigheden i.v.m. verzuim
        - Dossier van verzuimbegeleiding (gespreksverslagen, notities, plannen van aanpak, etc.)
        - Dossier van preventieve acties (gespreksverslagen, notities, etc.)
    - Medische gegevens (mogelijk; keuze klant voor daadwerkelijke vastlegging):
        - CAS- en CvO-codes, medische notities, verslagen, adviezen bedrijfsarts (en eventuele andere medische professionals).

- Van gebruikers:
    - Naam, e-mail, telefoonnummer (mobiel i.v.m. 2-factor authentication), aantal en momenten van inlog, uitgevoerde acties in dossiers.

DE DOELEINDEN VAN DE VERWERKING VAN DE PERSOONSGEGEVENS

- Van medewerkers:
    - Voldoen aan wettelijke eisen voor het opbouwen van arbodossiers (vanuit de arbowetgeving) van medewerkers die voldoen aan de eisen van het UWV (gesteld vanuit de Wet verbetering Poortwachter)

- Van gebruikers:
    - Noodzakelijk om te voldoen aan de eisen rondom privacy van medewerkers gesteld vanuit de Autoriteit Persoonsgegevens (vanuit de AVG).

AARD VAN DE VERWERKING VAN DE PERSOONSGEGEVENS

- Persoonsgegevens komen deels via automatische gegevensuitwisseling met personeelssysteem:
    1. Ontvangst op SFTP-server of via webservices Otherside at Work
    2. Conversie gegevens naar importstandaard Otherside at Work
    3. Verwerking gegevens in database Xpert Suite

- Handmatige verwerking:
    1. Toevoegen gegevens via webbrowser via beveiligde https-verbinding
    2. Verwerking in database Xpert Suite (gegevens worden geëncrypt opgeslagen)

Opschoning/ vernietiging gebeurt op basis van opdrachten van klant.

LANDEN WAAROP DEZE DIENSTEN GERICHT ZIJN

Deze diensten zijn gericht op Nederland.

Versie: Privacy & Security 2.1 checken bij versturen of dit de up-to-date versie is.

1 TABLE OF CONTENTS

2 INTRODUCTION

Otherside Software B.V. (Otherside) highly values the security of its customers' data, as well as the privacy rights of data subjects whose data is processed. The high standards that we set for this are reflected in physical, technical and procedural measures that we impose, adhere to and monitor both internally and also with respect to our suppliers.

This brochure gives you an impression of how Otherside interprets information security and privacy in all of its services and offerings, including from its offices in The Netherlands, Belgium and Sweden. If you have additional questions then of course please feel free to contact us at security@othersidesoftware.com for security questions or for privacy questions at privacy@othersidesoftware.com.

Furthermore, we would like to draw your attention to the ISO 27001 certificate, which Otherside obtained in October 2012, and the NEN7510[1] certificate which was obtained in September 2023. The management system used by Otherside to manage the risks around the availability and security of Xpert Suite is audited, certified and accredited in accordance with the international standard and the national standard.

The scope of Otherside's ISO 27001:2022 certificate is:

> *"All assets and processes related to the design, development, implementation and delivery of the software-services for 'occupational health management', 'professional performance of medical professionals' and for 'optimizing and automating of business processes in the manufacturing industry', as stated by the responsible management in the Statement of Applicability v4.0, dated 22-04-2024."*

The scope of Otherside's NEN 7510:2017 certificate is:

> *"All assets and processes related to the design, development, implementation and delivery of the software-services for 'occupational health management', and 'professional performance of medical professionals', as stated by the responsible management in the Statement of Applicability v4.0, dated 22-04-2024."*

In addition, Otherside is annually audited on its baseline of information security and privacy controls, after which an SOC2 type II report is issued.

[1] The Dutch Supervisory Authority (i.r.t. GDPR) considers the NEN7510 standard (which is based on the ISO27001 standard) to be an important standard for information security in healthcare.

3 SECURITY

3.1 Information Security Management System

Information security is managed via the ISO27001 and NEN7510 certified Information Security Management System (ISMS), registered via the BSI Group under certificate number ISC-077/NEN 7510-144. The administrator of the ISMS is the 'Information Security Officer'. One of the board-members also has the CISO-role and bears final responsibility for information security and privacy.

The management system is an integral part of the (annual) control cycle of the company as a whole:

- Each year, a risk analysis is performed on the basis of the experiences of the past year and developments within the environment (as part of the annual risk analysis Otherside also assesses whether sufficient measures have been taken to cover privacy risks);
- Based on the risk analysis, improvement plans are drawn up and submitted to the board for approval;
- After approval, the implementation of these points for improvement is monitored fully by the MT in the managing of the company.

As well as the management system itself, management processes are set up for which responsibilities are separated. Each process has someone with final responsibility who, in consultation with the board, determines when and on what controls take place. Whether or not each person responsible actually tackles his or her role is ultimately verified in the annual internal and external ISO audit. The controls/measures set up, as defined in ISO 27002/NEN7510-2, are all under management and controlled.

The following management processes have been established:

1. Access management
2. Asset management
3. Backup management
4. Capacity management
5. Change management
6. Compliance management
7. Continuity management
8. Customer management
9. Dataloss and malware protection
10. Incident management
11. Key management encryption
12. Logging management
13. Personnel management
14. Third party management
15. Vulnerability, Patch management & Hardening
16. Lifecycle Management

3.2 Organizational controls

3.2.1 Access control

There is a strict logical separation of the office environment (without customer data except for financial administration) and the production environment (with customer data). For this the following applies:

- The logical access to the office environment is managed operationally by workplace management. A printout of the active directory and the access rights on the various servers are checked annually.

- The joining and leaving protocol includes a checklist used to verify that all physical and logical access is closed. In addition, the checklist includes a number of other steps regarding the return of equipment and related items.
- Logical access to the production environment is screened separately.
- A limited number of employees have access to the production environment. This only if necessary for the performance of their own work
- Employees with access are given a personal user name and password, installed certificate and a second factor (time-based token) for an end-to-end VPN connection to the production environment.
- With an active VPN connection the employee can connect to a dedicated jump host with separate Active Directory credentials.
- Access to the servers for authorised employees is restricted depending on function. Only the servers necessary for their own work are accessible. Access to customer-environments is temporary for consultants (and only active during project work for specific customers).
- Access rights are actively updated in the event of job changes and leavers. The accuracy of the rights assigned is checked annually.
- Just as for all other users, access to production databases via the web interface is always secured with 2-factor authentication.

For the management of the servers on which the software and customer data are located, an employee also needs to be assigned a role defined in the Active Directory. This role assignment is kept up to date and checked periodically for accuracy. The standard windows mechanism is then used to restrict rights. Access to the management environment requires a VPN connection with certificates and 2-factor authentication.

Within the Xpert Suite, the customer administrators themselves can define and assign roles to users. Based on these roles, the software determines which changes users may and may not make. The basis of this authorisation is that the role determines what a user may do while the link to the employee files of the individual user determines for whom this is allowed. Taken together, these authorisations determine whether or not a change is permitted. Of course, in this context, all incoming changes are assessed by the server against the configured authorisations. Administrators can print out an IST matrix of the what authorisations and all the configured roles and have them tested internally (IST vs SOLL).

3.2.2 Incidents and non-conformities

Non-conformities can be established in a number of ways:

- During the annual internal audit;
- During the annual external ISO27001 / NEN7510 certification audit;
- During the annual SOC2 audit;
- As a result of the analysis of a reported incident.

Incidents can be reported by customers or employees or can be the result of a (periodic) audit of a control measure by a responsible contact person.

After a non-conformity has been established, an action plan is prepared. This action plan focuses on the question of what measures are necessary to remedy the non-conformity identified and to prevent it from recurring. A conclusion could be, for example, that the working methods in place are of such a sub-optimal nature that the temptation to bypass them is too great and that therefore modifications are necessary.

In order to monitor whether the measures taken have had the desired effect, for each measure, how and how often its effectiveness should be measured are explicitly defined. The responsible contact persons then implement the measures adopted. During the audit, all controls are checked to see whether this has been done.

Security incidents are discussed in the yearly knowledge session and, if caused by an individual or department, with the employees involved. When it is necessary to inform all employees immediately about security incidents (i.e. earlier than

the next annual knowledge session), a news message is sent internally. If a security incident leads to a (potential) data leak, the 'Duty to Report Data Leaks' procedure is followed. Within this procedure, data controllers need to be informed within 24 hours in accordance with the guidelines of the Dutch Supervisory Authority (related to the GDPR).

3.2.3 Independent review of information security

Audits are performed a number of times per year:

- Once per year, an internal audit, in which Otherside itself carries out checks on procedures of data controllers within the organisation. The results are discussed internally and improvement actions identified.
- Once per year, an external ISO 27001 / NEN7510 certification audit (once every 3 years an official certification and in between times a control audit each year). Based on these audits, a report is prepared and it is decided whether Otherside may retain the certificate.
- Once per year, an SOC2 audit performed by an external certified auditor. The auditor issues a signed declaration of the checks performed and the consequences for customers.

3.3 People controls

3.3.1 Awareness about information security

Once a year a knowledge session is planned examining the importance of information security for our customers and for the survival of our company. Posters and other visual aids are also used periodically to alert people to the procedures. The personnel manual also contains various guidelines regarding information security and refers actively to the information security policy.

3.3.2 Competencies

When someone joins the company and each year thereafter, an active assessment is made of whether the competencies of the individual are in line with the position held or whether any development is required. When competencies are no longer in line with the position, a change of position is a possibility. When personnel changes occur, an active assessment is made of whether the correct competencies are still present in the company or whether gaps have appeared. In the latter situation, we look at how these competencies within the organisation can be redeveloped or brought in.

3.3.3 Integrity

When hiring employees, a number of actions are performed to determine if the person is trustworthy when it comes to working with privacy-sensitive data:

- Diploma/reference check;
- Certificate of Good Behaviour (VOG) request;
- Signing of a declaration of confidentiality;
  Customer specific screenings.

3.3.4 Active assessment of working in line with information security policy

The extent to which an employee acts in accordance with the information security policy is part of the assessment interview. If an employee does not act properly in this respect, active warnings are given that can result in termination of employment. The self-reporting of any incident caused personally is assessed much less negatively than if another employee reports it. This is to create a culture where reporting an incident (even if it involves a mistake you made) is viewed as ‘positive’..

3.4 Physical controls

There is a strict physical separation of the office environment (without customer data except for financial administration) and the production environment (with customer data). For this the following applies:

- No employee of Otherside has independent physical access to the areas where customer data is stored. This always requires the cooperation of the hosting partner (Proserve) and the approval of the board.
- Proserve employees can physically access the equipment on which customer data is stored. However, this data is stored on encrypted disks and in encrypted databases, making the customer data unreadable for Proserve employees.
- The physical access to the office environment is recorded by the facility manager in a key plan and assessed annually. The areas covered in this key plan are: workstations (general), workstation financial administration, server room office environment (no customer data) and archive with administration.

The management of the physical and logical access is included in the access management procedure which in turn is part of the ISO27001/ NEN7510 certified ISMS.

3.4.1 Data location

The data is stored at the following locations:

Equinix AM3 *Science Park 610* *1098 XH Amsterdam*	*Dataplace Rotterdam* *Van Coulsterweg 6* *2952 CB Alblasserdam*	*Global Switch Amsterdam* *Johan Huizingalaan 759* *(entrance at Henk Sneevlietweg)* *1066 VH Amsterdam*

At all locations, the hardware is managed by sub-processor Proserve. Proserve is ISO27001, NEN7510, ISO9001 certified, and has a ISAE 3402 Type II assurance report.

Backup information is stored in both Equinix AM3 and Dataplace Rotterdam. Within Dataplace Rotterdam, the backups are stored at a separate room which is not accessible by Proserve nor internal Otherside-employees, unless one-time access is provided by the board of Otherside.

3.5 Technological controls

3.5.1 Network controls

All traffic to the production environment enters via a physical firewall whereby only traffic that has been explicitly opened and thus approved via the change procedures is allowed. The traffic is then routed over a segmented network whereby only the web and connection servers for which it is intended are accessible via the Internet.

DNS services are provided by a third party, protected by two factor logins and also monitored for changes with an independent external monitoring tool.

3.5.2 Network monitoring

Otherside has set up a SIEM that collects and analyses both the data traffic and the logging of actions carried out. This allows an additional assessment and active escalation if a user or software component performs 'unusual' actions.

3.5.3 use of cryptography

Web traffic is always secured via TLS, whereby the TLS settings are tested for known vulnerabilities using external tools. File exchanges take place via TLS or SFTP.

The database servers are not directly accessible and the databases are separated per customer. Stored data is encrypted by means of the TDE mechanism of SQL Server and in addition there is also cell level encryption for medical data entered by company doctors. The cell-level encryption takes place via the application with a customer and application key.
Also all Virtual Machines are stored on encrypted VMWare VSAN storage.

3.5.4 Logging

Mutations, exceptions, faults and other relevant events are generated and stored in logs and then analysed. The purpose of logging is to minimize disruptions, identify non-compliancy with the information security policy, generate evidence, and support investigations.
Centrally stored logs contain application error logs and security event logs. Logs concerning use of the Xpert Suite application are stored within Xpert Suite. These logs are protected against manipulation and are only accessible to authorised personnel.

The logs concerning the production environment are retained and backed-up for at least a year.

3.5.5 Backup & restore procedures

Otherside commits to optimal availability of Xpert Suite. To this end, backups are of customer data. We keep versions of backups depending on the duration:

- 7 daily back-ups;
- After 7 days, 1 of the daily backups is saved as a weekly backup. The other daily backups are deleted.
- After a month, 1 weekly backup is saved as a monthly backup and the other weekly backups are deleted;
- The monthly backups are deleted after 6 months.

This means that the oldest available backup is 5 to 6 months old. The backups are encrypted and periodically checked by means of restores.

Otherside has set up three backup locations. At the same location as the primary location for a customer, at the secondary location of a customer and at a dedicated cage in Dataplace which is not accessible by Proserve nor internal employees, unless one-time access is provided by the Board. This third location is using Veeam Insider Protection to prevent the possibility to delete the backups from the backup management server.

If the primary location is destroyed, the application will be available on the secondary location. If data is destroyed on both locations the data can be restored from the Veeam Insider Protection backup server and will be up-and-running within the period agreed in the SLA.

We apply a Recovery Point Objective (RPO) and Recovery Time Objective (RTO) of 24 hours for destruction of data at the primary site, meaning we aim for a maximum recovery time of 24 hours and data loss of 24 hours.

3.5.6 Software development

Otherside has incorporated Secure Development principles into its development methodology. For each individual change, the impact in terms of security is assessed in accordance with the requirements in the ISO27001 and NEN7510 guidelines. Developers use a checklist for this based on the OWASP top 10 guidelines, ISO27002 controls, NEN7510 controls, NCSC and NIST. For each release, the modified code is reviewed against this checklist and delivered to the Maintenance & Support department. Maintenance & Support then carries out a number of technical and functional acceptance tests, in which the operation of authorisations is tested before the new release goes into production.

At least once per year, an external party is asked to perform penetration tests on the software. The penetration test supplier is changed every 2 to 3 years to ensure a critical analysis. These tests are as of 2023 performed by Intigriti. In addition to the annual penetration test, at selected times throughout the year, a bug bounty program is active so that security researchers are motivated to look for vulnerabilities.

Sigrid CI is used for the assurance of Open Source Health and Security Issues in our code.

Secure programming competencies of developers are developed and kept up-to-date with the help of internal and external parties.

3.5.6.1 SECURITY & PRIVACY BY DESIGN AND DEFAULT

In the software design process, Otherside applies the following principles:

- When making a design, compliance with privacy legislation and the consequences for the data subjects are always included in the analysis;
- If a user has not made a choice for a particular setting then we use the strictest privacy settings (privacy by default);
- If users appear to be diverging from legal obligations then they always need to provide a reason for doing so (e.g. login without 2FA);
- At all points where the software can support users with regard to privacy-compliant operation, Otherside will try to provide a solution which is as user-friendly as possible, so that users follow this compliant working method as far as possible (e.g. not only SMS as 2FA, the Data Safe, DialoogXpert);
- The software supports the establishment of legal bases for processing for the purpose of supporting the data controller.

4 PRIVACY

Sensitive personal data is processed in the Xpert Suite. This means that the consequences for data subjects can be very great if errors are made in the processing. Ultimately, Otherside's customers are the data controllers for this processing but Otherside, with its procedures and measures, wants to offer a platform on which the controller can easily adhere to legal requirements and data subjects' rights. In doing so, we will direct our customers as much as possible towards a compliant working method.
The additional measures that Otherside has taken within the context of privacy legislation are listed below.

4.1 Processing agreement

Otherside enters into a processing agreement with all the customers who use its software. This agreement has been tested to ensure compliance with the relevant privacy legislation (in any case at least the GDPR). A standard processing agreement can be obtained from Otherside.

4.2 Sub-processors

For every customer that uses Xpert Suite, Proserve is used as a sub-processor (see 3.4.1).

The other sub-processors are only processing the data when the customer uses the mentioned specific functionality within Xpert Suite. The customer administrators can activate and agree to use these additional functions. These functions are purchased by the customer as an additional service and can be activated and de-activated by the customer administrator.

Sub-processor	Address	Functionality	Description
Proserve BV	Oostmaaslaan 71 3063 AN Rotterdam	Xpert Suite	The managing of hardware of XS data
CM.com	Nachtwachtlaan 20 1058 EA Amsterdam	SMS messages	Used for all SMS-messages sent from Xpert Suite, including; 1. Two-factor authentication codes; 2. Appointment reminders; 3. Links to questionnaires.
Microsoft Azure	Microsoft Datacenters in Western Europe and Sweden	SummarizeIT	Transcribing audio files or texts provided by users by using Large Language Models.
Telnyx Ireland Limited	Waterways House, 6th Floor Grand Canal Quay Dublin, D02 PD39 Ireland	SummarizeIT	VOIP Provider which produces audio files from a phone call so that SummarizeIT can transcribe it.

4.3 Data Protection Officer and privacy & security team

Otherside has put in place a Data Protection Officer and a privacy & security team. This privacy & security team consists of representatives from all parts of the organisation who potentially come into contact with customer data (consultants, support, IT management). In this consultation, all ongoing improvement actions, incidents and risk analyses are discussed, thus ensuring an integral monitoring of the security. The Data Protection Officer has been appointed to

supplement the impact in this consultation of improvement actions, incidents and risk analyses with consequences for data subjects.

The Data Protection Officer of Otherside is:

Jeroen van Woezik
E: privacy@othersidesoftware.com
T: 073 - 615 99 50

4.4 Data subjects contact

Otherside has set up a contact point for the data subjects which they can turn to with their questions. The basic rule is that a controller (i.e. the customer of Otherside) must communicate with the data subjects. But if this is not possible, Otherside wants to be accessible to data subjects and support them where possible in resolving any problems. Otherside can be reached by data subjects via:

E: loket.betrokkenen@othersideatwork.nl
T: 073 - 615 99 50

Information about this contact point is also available on the Otherside website. https://www.othersideatwork.nl/dit-is-otherside-at-work/privacy-statement

4.5 Retention periods

The data recorded in the Xpert Suite is subject to very different retention periods (for example, an employer must delete an absenteeism record within 2 years of the person concerned leaving the company while an occupational health and safety service must sometimes keep it for up to 40 years). Otherside has added functionality to its software that can be used as a customer to determine for themselves which periods should be used in which situation. This data, however, can still be present in the old versions of backups for 6 months. After that, the data is permanently deleted / destroyed.

This backup period is of this length due to long-running cases. Sometimes users are very late in discovering incorrectly deleted data. The rights of data subjects also include the obligation to retain data. Because backups are not operationally comprehensible, Otherside uses this period in weighing up the right to data destruction on the one hand against the right of retention on the other.

4.6 Legal requirements

Of course, Otherside cannot guarantee that every user of the Otherside software works in compliance with applicable laws and regulations. The responsibility for this remains with the controller.

BIJLAGE 3 BIJ VERWERKERSOVEREENKOMST MEDISCHE GEBRUIKERS

Contactgegevens

Voeg hieronder de contactgegevens toe van de contactpersonen namens de Verwerkingsverantwoordelijke voor de verwerking van medische gebruikers in de XS tenant van Opdrachtgever. Deze contactpersonen worden gecontacteerd als Otherside at Work (Verwerker) verzocht wordt om toegang tot medische gegevens aan te passen voor gebruikers. De security contactpersonen worden geïnformeerd over wijzigingen aan maatregelen of voor datalek-meldingen en security-incidenten op de XS tenant van Opdrachtgever voor zover het medische gegevens betreft.

Delegate Medical Contracteigenaar en vertegenwoordiger verwerkingsverantwoordelijke	
**Naam*	
**Email*	
**Telefoon*	
**Mobiel*	

Delegate Medical Eventueel gedelegeerd vertegenwoordiger	
**Naam*	
**Email*	
**Telefoon*	
**Mobiel*	

Security Contact Medical Functionaris gegevensbescherming of data protection officer medische gegevens	
**Rol*	
**Naam*	
**Email*	
**Telefoon*	
**Mobiel*	

Security Contact Medical Functionaris gegevensbescherming of data protection officer medische gegevens	
**Rol*	
**Naam*	
**Email*	
**Telefoon*	
**Mobiel*	

** Graag digitaal dan wel schriftelijk aan te vullen door Verwerkersverantwoordelijke.*

Voor het doen van een incident- of datalekmelding als KLANT aan Otherside at Work:

Xpert Desk Otherside at Work
xpertdesk@othersideatwork.com
+31 73 615 99 99

Daarnaast kan contact opgenomen worden met de functionaris gegevensbescherming (FG) en/of de information security officer (ISO) van Otherside at Work.

FG	ISO
privacy@othersidesoftware.com	security@othersidesoftware.com
+31 73 615 9950 (kantoortijden)	+31 73 615 9950 (kantoortijden)