GEBRUIKERSOVEREENKOMST
XPERT SUITE DATAKLUIS

USER AGREEMENT
XPERT SUITE DATA SAFE

OTHERSIDE AT WORK

VERSIE / VERSION	4.2
STATUS	Definitief / Final
DATUM / DATE	18-05-2022
CLASSIFICATIE / CLASSIFICATION	Openbaar / Public

ENGLISH VERSION WILL FOLLOW BELOW DUTCH TEXT

De besloten vennootschap met beperkte aansprakelijkheid **Otherside at Work B.V.**, gevestigd en kantoorhoudende aan de Wisent 14 te 's-Hertogenbosch (5236 PX) (hierna te noemen: "**Otherside**") verleent hierbij aan Afnemer (zoals hierna gedefinieerd) het recht om de Datakluis onder de volgende voorwaarden te gebruiken. Gezamenlijk hierna te noemen Partijen.

Partijen nemen het volgende in overweging:
De Datakluis is ontwikkeld om werkgevers te ondersteunen in het veilig en in lijn met privacyregels delen van persoonsgegevens van zijn medewerkers met arbodiensten en andere verzuimdienstverleners ("Dienstverleners"). Hierbij zorgt de Datakluis ervoor dat:

- Werkgevers een eenvoudig werkproces houden bij het doorgeven van verzuimmeldingen aan Dienstverleners
- De datakwaliteit beter wordt gewaarborgd: niet per ongeluk omwisselen of splitsen van dossiers
- De Dienstverlener verzuimanalyses over uw medewerker populatie kan uitvoeren en rapporteren
- De Dienstverlener de mogelijkheid krijgt om de wettelijke verplichte anonieme spreekuren te ondersteunen met behoud van datakwaliteit en zonder indirect de werkgever hier inzicht in te geven

De Datakluis kan zowel worden ingezet in de situatie waar de werkgever handmatig persoonsgegevens en verzuimmeldingen doorgeeft aan de Dienstverlener, als in de situatie dat dit via een geautomatiseerde gegevensuitwisseling plaatsvindt.

De Datakluis zorgt er in beide situaties voor dat de werkgever de persoonsgegevens in zijn eigen Datakluis plaatst, waarna alleen in toegestane situaties de juiste gegevens naar de Dienstverlener worden doorgegeven. Hierbij bestaan de volgende gegevensstromen richting de Dienstverlener:

- Gepseudonimiseerde gegevens van de medewerkerspopulatie worden direct doorgegeven aan de Dienstverlener. Hierdoor weet een Dienstverlener wel hoeveel werknemers, FTE, afdelingen en functies er aanwezig zijn in de organisatie, maar niet welke personen dat zijn. Elke mutatie in deze populatie wordt gepseudonimiseerd doorgegeven, zodat deze getallen voor de Dienstverlener altijd actueel zijn.

- Wanneer er een zorgvraag is voor een specifieke medewerker, dan wordt voor die ene medewerker het bij de Dienstverlener aanwezige gepseudonimiseerde record aangevuld met persoonsgegevens, waardoor de Dienstverlener conform de wettelijke eisen haar eigen dossier kan gaan opbouwen.

Tevens kan de Dienstverlener handmatig persoonsgegevens uit de Datakluis opvragen van een medewerker die op een inloopspreekuur komt. Op basis van een combinatie van de opgevoerde gegevens (in ieder geval werkgever, postcode en geboortedatum) kan de Datakluis teruggeven welk gepseudonimiseerd record bij deze werknemer hoort, zodat bij een eventuele toekomstige verzuimmelding de Dienstverlener wel over het complete persoonsdossier beschikt. Deze matching blijf verborgen voor de werkgever, zodat ook hier aan de geldende privacyrichtlijnen en arbowetgeving wordt voldaan.

De gegevens in de Datakluis worden door Otherside als verwerker verwerkt namens de verwerkingsverantwoordelijke Werkgever en betreffen alleen de volgende noodzakelijke gegevens:

- Werkgever
- Naam (alle delen van de eigen naam en partnernaam en voorkeurshantering)
- Geslacht
- Geboortedatum

Daarnaast kunnen de volgende optionele gegevens met de Datakluis verwerkt worden:

- Personeelsnummer
- Adresgegevens (inclusief postcode, woonplaats, land)
- Contactgegevens (telefoonnummers, e-mailadressen, bankrekeninggegevens)
- BurgerServiceNummer

De gegevens die gedeeld worden met de Dienstverlener worden niet meer in de Datakluis verwerkt en vallen buiten deze gebruikersovereenkomst. Hiervoor is een aparte overeenkomst tussen de Dienstverlener en Otherside voor het gebruik van de 'Xpert Suite'.

Deze gebruikersovereenkomst en bijbehorende voorwaarden zijn tevens de verwerkersovereenkomst in de zin van de AVG.

Partijen komen het volgende in overeen:

1 Definities
In deze Leveringsovereenkomst worden de volgende begrippen gebruikt:

1.1 Afnemer: De entiteit (werkgever) die gebruik maakt van de DataKluis en daarin Persoonsgegevens (personeelsgegevens) zet en Eindgebruikers kan autoriseren voor gebruik van de DataKluis.

1.2 Aanvullende Nationale Wetgeving: de nationale wetgeving met betrekking tot de verwerking van Persoonsgegevens in een lidstaat van de EU naast de AVG.

1.3 AVG: Algemene Verordening Gegevensbescherming: wet die sinds 25 mei 2018 van kracht is. Deze wet zorgt ervoor dat in de hele Europese Unie (EU) dezelfde privacywetgeving geldt. De AVG is ook wel bekend onder de Engelse naam: General

Data Protection Regulation (GDPR). Op een aantal punten laat de AVG-ruimte voor nationale keuzes, deze zijn uitgewerkt in de UAVG.

1.4 Betrokkene degene wiens Persoonsgegevens worden verwerkt en hun recht als Betrokkene kunnen uitoefenen.

1.5 Beveiligingsinbreuk: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

1.6 Colocaties: Externe locaties waar Otherside de technische infrastructuur van de Datakluis dienst heeft ondergebracht.

1.7 Datakluis: de Xpert Suite Datakluis dienst van Otherside.

1.8 Dienstverlener: commerciële en/of niet-commerciele bedrijfsgezondheidsdienst zoals maar niet uitsluitend arbodienstverleners, schadelastbeheersers, casemanagementbedrijven en/of bedrijfsartsennetwerken die gebruik maken van Xpert Suite.

1.9 Leveringsovereenkomst: deze gebruikersovereenkomst tussen Afnemer en Otherside met betrekking tot het gebruik van de Datakuis en de verwerking van de daarin door de Afnemer opgeslagen (persoons)gegevens.

1.10 Licentie: het recht om de Xpert Suite Datakluis te gebruiken.

1.11 Licentievoorwaarden: de op deze Leveringsovereenkomst van toepassing zijnde Xpert Suite Licentievoorwaarden van Otherside.

1.12 Persoonsgegevens: alle informatie over een geidentificeerd of identificeerbaar natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat (*direct Persoonsgegeven*), ofwel naar deze persoon te herleiden is (*indirect Persoonsgegeven*). Hierbij wordt onderscheid gemaakt tussen Persoonsgegevens en Bijzondere Persoonsgegevens. Persoonsgegevens zijn bijvoorbeeld iemands naam, adres en woonplaats, maar ook telefoonnummers en postcodes met huisnummers zijn Persoonsgegevens. Bijzondere Persoonsgegevens zijn gegevens over iemands: ras/ etnische afkomst; politieke opvattingen; godsdienst / levensovertuiging; lidmaatschap vakbond; genetische / biometrische gegevens met oog op unieke identificatie; gezondheid; seksuele leven; strafrechtelijk verleden. Een organisatie mag geen bijzondere Persoonsgegevens verwerken, tenzij daarvoor in de wet een uitzondering is.

1.13 Otherside: Otherside at Work B.V.

1.14 Software: DataKluis.

1.15 Toezichthoudende Autoriteit: door een lidstaat aangewezen onafhankelijke overheidsinstantie die verantwoordelijk is voor het toezicht op de landelijke toepassing van de UAVG. Otherside is gebonden aan de Nederlandse Toezichthoudende Autoriteit, te weten de Autoriteit Persoonsgegevens.

1.16 Toepasselijke Privacy Wetgeving: AVG, UAVG en de Aanvullende Nationale Wetgeving.

1.17 Verwerken (van Persoonsgegevens): alle handelingen met betrekking tot Persoonsgegevens, van verzamelen tot en met vernietigen. Handelingen die er volgens de AVG in ieder geval onder vallen zijn: het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen van Persoonsgegevens.

1.18 UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming. Wet van 16 mei 2018, houdende regels ter uitvoering van 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 en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).

1.19 Verwerken (van Persoonsgegevens): alle handelingen met betrekking tot Persoonsgegevens, van verzamelen tot en met vernietigen. Handelingen die er volgens de AVG in ieder geval onder vallen zijn: het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen van Persoonsgegevens.

1.20 Pseudonimiseren: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. Gepseudonimiseerde persoonsgegevens vallen onder de AVG.

1.21 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt.

1.22 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

2 Algemeen

2.1 Voor zover enige bepaling van deze Leveringsovereenkomst in strijd is met hetgeen in de Licentievoorwaarden is bepaald, prevaleert hetgeen in deze Leveringsovereenkomst is bepaald.

2.2 Deze Leveringsovereenkomst bevat ook de afspraken welke dienen te worden vastgelegd in

een 'verwerkersovereenkomst' zoals omschreven in de AVG.

3 Gebruik van de Datakluis

3.1 Op voorwaarde van volledige naleving van de voorwaarden uit deze Leveringsovereenkomst en de toepasselijke Licentievoorwaarden verleent Otherside hierbij aan Afnemer een niet-exclusieve, niet-sublicentieerbare en niet-overdraagbare Licentie.

3.2 Voor het gebruik van de Datakluis is geen gebruiksvergoeding verschuldigd en staat los van het contract dat u met uw Dienstverlener heeft. Het kan zijn dat de Dienstverlener vanwege de wijzigingen op dit gebied separaat kosten voor de maatregelen die zij moeten treffen in het kader van security en compliancy met u overeenkomt en aan u doorbelast.

3.3 Afnemer bepaalt welke gegevens met behulp van de Datakluis wordt opgeslagen en/of uitgewisseld. Otherside heeft geen semantische kennis van die gegevens en heeft uitsluitend toegang voor beheer en onderhoud van de Datakluis. Afnemer is er dan ook verantwoordelijk voor dat die gegevens rechtmatig zijn en geen inbreuk maakt op rechten van derden. Afnemer vrijwaart Otherside voor aanspraken van derden die gebaseerd zijn op de stelling dat de door Afnemer met behulp van de Datakluis opgeslagen en/of uitgewisselde data of informatie onrechtmatig is. Mocht Otherside kennis hebben of tot het besef komen dat data of informatie die Afnemer met behulp van de Datakluis heeft opgeslagen en/of uitgewisseld onrechtmatig is, dan behoudt Otherside zich het recht voor om de gegevens in quarantaine te plaatsen door de toegang daartoe onmogelijk te maken. Otherside zal, als de rechtmatigheid niet alsnog kan worden aangetoond binnen 2 weken, deze gegevens definitief verwijderen. In geen geval zal Otherside aansprakelijk zijn voor schade die voortvloeit uit dat handelen.

4 Opslag en verwerking van (persoons)gegevens in de Datakluis

4.1 Het gebruik van de Datakluis brengt verwerkingen van (bijzondere) Persoonsgegevens met zich mee. Afnemer wordt beschouwd als de Verwerkingsverantwoordelijke. Dit betekent dat de verantwoordelijkheid voor naleving van de Toepasselijke Privacy Wetgeving bij het verwerken van Persoonsgegevens bij Afnemer ligt. Otherside fungeert hierbij als Verwerker.

4.2 De volgende gegevens worden vastgelegd in de Datakluis en worden dus niet doorgegeven naar de Dienstverlener totdat er een concrete zorgvraag is:

- Naam (alle delen van de eigen naam en partnernaam)
- Adresgegevens (inclusief postcode, woonplaats, land)
- Contactgegevens (telefoonnummers, e-mailadressen, Bankrekeninggegevens)
- Geboortedatum
- Burger Service Nummer (eventueel)

5 Opvolgen van opdrachten en instructies door Otherside

5.1 Het is niet toegestaan dat Otherside Persoonsgegevens voor eigen doeleinden gaat verwerken en/of aan derden te verstrekken.

5.2 Otherside verwerkt gegevens ten behoeve van Afnemer, overeenkomstig diens instructies en onder diens verantwoordelijkheid. Afnemer is Verwerkingsverantwoordelijke.

5.3 Otherside heeft geen zeggenschap over het doel en de middelen voor de verwerking van de Persoonsgegevens. Zo neemt Otherside geen beslissingen over de ontvangst en het gebruik van de Persoonsgegevens, de verstrekking aan derden en de duur van de opslag van de Persoonsgegevens. De zeggenschap over de Persoonsgegevens komt nimmer bij Otherside te berusten.

5.4 Naast de verplichting van Otherside om de instructies van Afnemer te volgen, dient Otherside ook zorg te dragen voor de naleving van de voorwaarden die met name op grond van de AVG worden gesteld aan het verwerken van Persoonsgegevens.

5.5 Als de Toezichthoudende Autoriteit audits, inspecties of onderzoekingen verricht bij de Afnemer verband houdende met deze Leveringsovereenkomst zal Otherside zijn volledige medewerking verlenen.

5.6 Als de Autoriteit Persoonsgegevens audits, inspecties of onderzoekingen verricht bij Otherside stelt Otherside de Afnemer onmiddellijk schriftelijk op de hoogte hiervan (met uitzondering van dwingendrechtelijk verbod). Daarnaast stelt Otherside de Afnemer op de hoogte van alle bevindingen van de Autoriteit Persoonsgegevens die direct of indirect effect zullen hebben op deze overeenkomst.

5.7 Otherside zal de aanbevelingen van de Autoriteit Persoonsgegevens betrekking hebbende op deze Leveringsovereenkomst onmiddellijk opvolgen.

5.8 Otherside zal een verzoek tot inzage, wijziging, dataportabiliteit, verwijdering van Persoonsgegevens, intrekking van toestemming verwerking van Persoonsgegevens of beperking van verwerking van Persoonsgegevens (Recht van Betrokkene) binnen 5 werkdagen doorsturen naar de Afnemer en zal alle medewerking verlenen aan de Afnemer bij een dergelijk verzoek.

5.9 Otherside zal op verzoek van Afnemer medewerking verlenen aan een gegevensbeschermingseffect- beoordeling (Data Protection Impact Assessment (DPIA)).

6 Beveiligingsmaatregelen

6.1 Otherside neemt alle passende technische en organisatorische maatregelen om de Persoonsgegevens te beveiligen tegen verlies, vernietiging of

enige vorm van onrechtmatige verwerking. 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. Deze maatregelen zijn in ieder geval gericht om:

1. Te voorkomen dat onbevoegden toegang krijgen tot systemen waarin de Persoonsgegevens worden verwerkt.
2. Te voorkomen dat systemen waarin de Persoonsgegevens worden verwerkt zonder toestemming worden gebruikt.
3. Ervoor te zorgen dat alleen de daartoe bevoegde personen de Persoonsgegevens mogen Verwerken in de betreffende systemen en dat de Persoonsgegevens niet kunnen worden Verwerkt zonder toestemming van de Afnemer.
4. Ervoor te zorgen dat de Persoonsgegevens niet kunnen worden gelezen, gekopieerd, veranderd of verwijderd zonder toestemming van de Afnemer tijdens digitale overdracht of opslaan van de Persoonsgegevens.
5. Ervoor te zorgen dat het te traceren is welke Persoonsgegevens, in de systemen waarin zij worden verwerkt zijn aangemaakt, gewijzigd of verwijderd en door wie.
6. Ervoor te zorgen dat alle passende technische en organisatorische maatregelen om de Persoonsgegevens te beveiligen tegen verlies, vernietiging of enige vorm van onrechtmatige verwerking worden nageleefd door de (sub)verwerkers van Otherside.
7. Ervoor te zorgen dat de Persoonsgegevens verzameld voor verschillende doeleinden afzonderlijk kunnen worden verwerkt.

6.2 Otherside zal, in het kader van de in het vorige sublid beschreven verplichting, tenminste de in de 'Privacy and Security Controls Otherside at Work' gespecificeerde maatregelen treffen.

6.3 De door Otherside in dit kader te nemen maatregelen zullen in ieder geval voldoen aan het ISO27001 normenkader, waarvoor Otherside jaarlijks door een certificerende instantie ge-audit wordt.

7 Verantwoordingsplicht

7.1 Otherside voorziet de Afnemer van de noodzakelijke informatie waardoor de Afnemer een oordeel kan vormen over de naleving door Otherside van deze overeenkomst.

7.2 Otherside licht op eerste verzoek van de Afnemer de opzet en werking toe van het stelsel van maatregelen en procedures, gericht op de naleving van deze overeenkomst.

7.3 De Afnemer heeft met betrekking tot de eigen Persoonsgegevens het recht om de technische en organisatorische beveiligingsmaatregelen die Otherside heeft getroffen te onderzoeken gedurende de duur van deze overeenkomst. In dit kader heeft de Afnemer het recht om alle relevante rapporten over IT-beveiliging of privacy audits op te vragen bij de Otherside. Daarnaast heeft de Afnemer het recht om audits uit te voeren over de Persoonsgegevens verwerkingen door Otherside. Otherside zal de Afnemer alle nodige informatie verschaffen voor het uitvoeren van deze audits.

7.4 Op verzoek kan de Afnemer een security audit (laten) uitvoeren op de relevante generieke infrastructuur, klantspecifieke infrastructuur en het informatiebeveiligingsbeleid van Otherside door daartoe gekwalificeerde medewerkers en/of derden. Een audit die zal plaatsvinden op de infrastructuur en systemen die voor meerdere klanten worden ingezet is toegestaan, mits de belangen van deze klanten niet geschaad worden. Dit zal vooraf door Otherside worden bepaald. Otherside en haar(sub)verwerkers zullen de auditors die optreden namens de Afnemer met betrekking tot een audit voorzien van alle redelijke medewerking en toegang tot de faciliteiten waar Persoonsgegevens verwerkt worden. Dit geldt voor zowel een audit op de infrastructuur en/of informatiesystemen als op de kantoren van Otherside en Colocaties. Op de Colocaties is Otherside afhankelijk van de medewerking van de desbetreffende dienstverleners en/of leveranciers. Wanneer hiertoe aanleiding is, zal Otherside zelf een opdracht geven tot het uitvoeren van een security audit.

7.5 De benodigde medewerking door Otherside en/of haar (sub)verwerkers aan een audit en de kosten hiervan worden aan de Afnemer doorbelast. Otherside verstrekt alle informatie die Afnemer nodig heeft voor het zelf uitvoeren van een gegevensbeschermingeffectbeoordeling, maar zal kosten doorbelasten indien Afnemer ondersteuning nodig heeft bij het uitwerken van de gegevensbeschermingeffectbeoordeling.

8 Medewerkers en Subverwerkers

8.1 Als Otherside voor het verwerken van de Persoonsgegevens een derde inschakelt (hierna te noemen "subverwerker") zal Otherside de Afnemer vooraf informeren. Otherside draagt er zorg voor dat alle verplichtingen uit deze Leveringsovereenkomst eveneens gelden voor (sub)verwerker.

8.2 De verplichtingen van Otherside die uit deze Overeenkomst voortvloeien, gelden ook voor degenen die de Persoonsgegevens verwerken onder het gezag van Otherside en/of (sub)verwerker.

8.3 Ter invulling hiervan zal Otherside in ieder geval deze personen verplichten, met uitzondering van dwingendrechtelijke verplichtingen, tot geheimhouding van de Persoonsgegevens waarvan zij uit hoofde van de verbintenis met Otherside kennisnemen.

8.4 Afnemer autoriseert Otherside hierbij om hostingpartner Proserve BV te betrekken als sub-verwerker

op de Colocaties.

9 Datalekken

9.1 In het geval van een datalek als bedoeld in artikel 33 AVG respectievelijk een inbreuk op de beveiliging als bedoeld in artikel 32 AVG of enig ander incident met betrekking tot de Persoonsgegevens, zal Otherside direct, maar in ieder geval binnen 24 uur na het ontdekken van het datalek, de Afnemer daarover informeren op het opgegeven mailadres bij goedkeuren van deze overeenkomst. Otherside garandeert dat de verstrekte informatie volledig, correct en accuraat is voor zover Verwerker dat op dat moment redelijkerwijs kan vaststellen. Zodra in een latere fase aanvullende relevante informatie over het datalek (of inbreuk op de beveiliging) bekend is zal Otherside Afnemer hierover nader informeren op het opgegeven emailadres.

9.2 De meldplicht geldt ongeacht de omvang en impact van het datalek.

9.3 De meldplicht van Otherside aan de Afnemer behelst in ieder geval het melden van het feit dat er een datalek is geweest, alsmede het melden van:
- de (mogelijke) oorzaak (oorzaken) van het datalek;
- de (vooralsnog bekende en/of te verwachten) gevolg(en) van het datalek;
- de (voorgestelde) oplossing(en);
- de contactgegevens binnen de organisatie van Otherside voor de opvolging van de melding;
- de reeds getroffen maatregelen om herhaling te voorkomen.

10 Looptijd, Wijziging en beëindiging overeenkomst

10.1 De Leveringsovereenkomst wordt aangegaan vanaf het moment van activatie van de Datakluis.

10.2 De Leveringsovereenkomst geldt voor onbepaalde tijd.

10.3 Wanneer Afnemer de samenwerking met haar Dienstverlener beëindigt en/of Dienstverlener de samenwerking met Otherside beëindigt wordt deze Leveringsovereenkomst beëindigd.

10.4 De Leveringsovereenkomst kan slechts schriftelijk en met instemming van Partijen worden gewijzigd.

10.5 Als door een wijziging van wet- of regelgeving een artikel uit deze Leveringsovereenkomst niet meer (onverkort) geldig is, zullen Partijen in onderling overleg een vervangend artikel overeenkomen dat zoveel mogelijk recht doet aan de strekking van het originele artikel.

10.6 Partijen hebben het recht om de Leveringsovereenkomst te beëindigen. Dit dient schriftelijk te worden aangegeven.

10.7 Zodra conform Artikel 10.3 de Afnemer de samenwerking met haar Dienstverlener beëindigt en/of de Dienstverlener de samenwerking met Otherside beëindigt wordt de Datakluis gedeactiveerd. Dat wil zeggen, alle data in de Datakluis wordt vernietigd en de Datakluis is niet meer beschikbaar.

10.8 Verplichtingen uit deze Leveringsovereenkomst die naar hun aard voortduren na beëindiging van de overeenkomst, blijven onverminderd van kracht.

10.9 De Afnemer is gerechtigd de Leveringsovereenkomst met onmiddellijke ingang op te zeggen ingeval Otherside zich niet houdt aan de in deze Leveringsovereenkomst aangegane verplichtingen.

10.10 Elk van de Partijen is gerechtigd de Leveringsovereenkomst met onmiddellijke ingang te beëindigen ingeval van overmacht, waaronder mede wordt begrepen een zodanige wijziging van de wettelijke regels dat een verdere voortzetting van de Leveringsovereenkomst redelijkerwijs niet kan worden verlangd.

10.11 Zodra de samenwerking is beëindigd, wordt de Datakluis gedeactiveerd (conform toelichting in artikel 10.7), tenzij Partijen iets anders overeenkomen of als langere bewaring noodzakelijk is op grond van wet- of regelgeving dan wel om te kunnen voldoen aan de verplichtingen die nog uit de samenwerking voortvloeien. Bij Afnemer ligt het initiatief om voorafgaand aan het beëindigen van de samenwerking met Otherside hierover afspraken te maken, ook over het ontvangen van een schriftelijke bevestiging van het vernietigen van de Persoonsgegevens van Afnemer.

11 Aansprakelijkheid

11.1 In aanvulling op artikel 6 van de Licentievoorwaarden geldt dat indien er als gevolg van een toerekenbare tekortkoming van Otherside, of een aan Otherside toerekenbaar gedraging of nalaten, door een overheidstoezichthouder aan Afnemer een boete wordt opgelegd, welke boete (deels) rechtstreeks verband houdt met voornoemde tekortkoming, gedragen of nalaten, vrijwaart Otherside Afnemer voor (dat deel van) die boete. De vrijwaring geldt niet voor zover de boete (mede) verband houdt met gedrag van Afnemer zelf of wanneer Afnemer zelf redelijkerwijs maatregelen had kunnen nemen om de boete te voorkomen. Op deze vrijwaring zijn de beperkingen van aansprakelijkheid van toepassing conform de Licentievoorwaarden.

ENGLISH VERSION

The private company with limited liability **Otherside at Work B.V.**, having its registered office and place of business at Wisent 14 in 's-Hertogenbosch (5236 PX) (hereinafter referred to as: "**Otherside**") hereby grants the Customer (as defined below) the right to use the Data Safe subject to the following terms and conditions. The parties are jointly referred to below as 'the Parties'.

The Parties take the following into consideration:
The Data Safe was developed to support employers in sharing personal data of its employees with ar-services and other absence service providers ("Service Providers") securely and in line with privacy regulations. In doing so, the Data Safe ensures that:

- Employers maintain a simple work process when passing on sickness reports to Service Providers
- Data quality is better ensured: no accidental swapping or splitting of files
- The Service Provider can conduct and report absence analyses on your employee population
- The Service Provider can support legally required anonymous consultation hours while maintaining data quality and without indirectly giving the employer insight into this

The Data Safe can be used both in the situation where the employer manually transmits personal data and absence reports to the Service Provider, and in the situation where this is done through automated data exchange.

In both situations, the Data Safe ensures that the employer places the data in its own Data Safe, after which the correct data are transferred to the Service Provider only in legally authorised situations. the following data flows exist towards the Service Provider:

- Pseudonymised data of the employee population are transmitted directly to the Service Provider. As a result, while a Service Provider knows how many employees, FTE, departments and positions are present in the organisation, it does not know which individuals they are. Any movement in this population is transmitted pseudonymised, so that these numbers are always up to date for the Service Provider.
- When there is a request for care for a specific employee, the pseudonymised record present at the Service Provider is supplemented with personal data for that one employee, allowing the Service Provider to start building its own file in accordance with legal requirements.

The Service Provider may also manually retrieve personal data from the Data Safe from an employee who attends a walk-in clinic. Based on a combination of the data entered (at least employer, postcode and date of birth), the Data Safe can return which pseudonymised record belongs to this employee, so that in the event of any future absenteeism report, the Service Provider does have the complete personal file. This matching remains hidden from the employer, ensuring compliance with applicable privacy guidelines and health and safety legislation here as well.

The data in the Data Safe is processed by Otherside as a processor on behalf of the controller (Employer) and only involve the following necessary data:.

- Employer
- Employee name (all parts of it)
- Sex
- Birth date

In addition, the following optional data can be processed in the Data Safe:

- Employee number
- Address data (including postal code, country and residence)
- Contact details (phone number, email address, bank account numbers)
- BurgerServiceNummer

Data shared with the Service Provider is no longer processed in the Data Vault and is outside of this user agreement. For this, there is a separate agreement between the Service Provider and Otherside for the use of the 'Xpert Suite'.

This user agreement and associated terms are also the processor agreement within the meaning of the AVG.

The Parties agree as follows:

1 Definitions
The terms below are defined as follows in this Supply Agreement:

1.1 Customer The entity (employer) that uses the Data Safe and puts Personal Data (personnel data) in it and can authorise End Users to use the Data Safe.

1.2 Supplementary National Legislation: the national legislation relating to the processing of Personal Data in a Member State of the EU that applies in addition to the GDPR.

1.3 GDPR: General Data Protection Regulation: law in force since 25 May 2018. This law ensures that the same privacy laws apply throughout the European Union (EU). On a number of points, the GDPR leaves room for national choices; these are de-

tailed in the Dutch General Data Protection Regulation (Implementation) Act.

1.4 Data Subject the person whose Personal Data are processed and can exercise their right as a Data Subject.

1.5 Security Incident: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.6 Colocation Data Centres: Remote locations where Otherside has hosted the technical infrastructure of the Data Safe service.

1.7 Data Safe: the Xpert Suite Data Safe service from Otherside.

1.8 Service Provider: Commercial and/or non-commercial occupational health and safety services, including, but not limited to, OHSS providers, claims managers, case management companies, and/or occupational physician networks who use Xpert Suite.

1.9 Supply Agreement: this user agreement between the Customer and Otherside for the use of the Data Safe and processing of the personal and other data that the Customer stores in it.

1.10 Licence: the right to use the Xpert Suite Data Safe.

1.11 Licence Terms: the Xpert Suite Licence Terms of Otherside applicable to this Supply Agreement.

1.12 Personal Data: any information relating to an identified or identifiable natural person. This means that information is either directly about someone (*direct Personal Data*) or traceable to them (*indirect Personal Data*). This distinguishes between Personal Data and special Personal Data. Personal Data are, for example, a person's name, address and place of residence, but also telephone numbers and postcodes with house numbers. Special Personal Data are data on a person's: racial/ethnic origin; political opinions; religion/beliefs; trade union membership; genetic/biometric data for the purpose of unique identification; health; sex life; criminal record. An organisation may not process special Personal Data unless there is an exception for this in the law.

1.13 Otherside: Otherside at Work B.V.

1.14 Software: Data Safe.

1.15 Supervisory Authority: independent public authority designated by a Member State responsible for monitoring the national application of the GDPR(I)A. Otherside is bound by the Dutch Supervisory Authority, namely the Dutch Personal Protection Authority.

1.16 Applicable Privacy Legislation: GDPR, GDPR(I)A and the Additional National Legislation.

1.17 Processing (of Personal Data): all operations concerning Personal Data, from collection to destruction. Actions that it covers under the GDPR in any case include: the collection, recording, organisation, structuring, storage, updating or modification, retrieval, consultation, use, transmission, dissemination, making available, association, blocking, erasure and destruction of Personal Data.

1.18 GDPR(I)A: General Data Protection Regulation (Implementation) Act. Act of 16 May 2018, containing rules to implement Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (general data protection regulation) (OJEU 2016, L 119).

1.19 Pseudonymisation: processing personal data in such a way that the personal data can no longer be linked to a specific data subject without the use of additional data, provided that such additional data are kept separately and technical and organisational measures are taken to ensure that the personal data are not linked to an identified or identifiable natural person. Pseudonymised personal data are covered by the GDPR.

1.20 Processor: a natural person or legal entity, public authority, agency or other body who/that processes personal data on behalf of the Controller.

1.21 Controller: a natural person or legal entity, public authority, agency or other body who/that, alone or jointly with others, determines the purposes and means of the processing of personal data.

2 General

2.1 If any provision of this Supply Agreement is inconsistent with the provisions of the Licence Terms, the provisions of this Supply Agreement take precedence.

2.2 This Supply Agreement also contains the arrangements that must be documented in a 'processing agreement' as described in the GDPR.

3 Use of the Data Safe

3.1 Subject to full compliance with the terms of this Supply Agreement and the applicable Licence Terms, Otherside grants the Customer a non-exclusive, non-sublicensable, and non-transferable Licence.

3.2 There is no user fee for using the Data Safe and it is separate from the contract you have with your Service Provider. Because of the changes in this area, the Service Provider can agree separate costs with you for the measures they have to adopt for the purpose of security and compliance and pass these costs on to you.

3.3 The Customer determines which data are stored and/or exchanged using the Data Safe. Otherside has no semantic knowledge of those data and has access only for managing and maintaining the Data Safe. The Customer is therefore responsible for ensuring those data are lawful and do not infringe third-party rights. The Customer indemnifies Otherside against third-party claims based on the assertion that the data or information that the Customer has stored and/or exchanged using the Data Safe is unlawful. If Otherside knows or realises

that data or information that the Customer stores and/or exchanges using the Data Safe is unlawful, Otherside reserves the right to quarantine and make access to the data impossible. Otherside will permanently delete these data if their lawfulness cannot be proven within two weeks. Otherside will never be liable for any damage resulting from such actions.

4 Storage and processing of personal and other data in the Data Safe

4.1 The use of the Data Safe involves processing special and other Personal Data. The Customer is regarded as the Controller. This means that responsibility for compliance with the Applicable Privacy Legislation when processing Personal Data lies with the Customer. Otherside acts as the Processor in this regard.

4.2 The following data are recorded in the Data Safe and are therefore not passed on to the Service Provider until there is a concrete request for care:

- Name (all parts of own name and partner's name)
- Address details (including postcode, city, country)
- Contact details (phone numbers, email addresses, bank account details)
- Date of birth
- Citizen Service Number (if any)

5 Otherside's compliance with orders and instructions

5.1 Otherside must not process Personal Data for its own purposes and/or disclose them to third parties.

5.2 Otherside processes data on behalf of the Customer in accordance with the Customer's instructions and under the Customer's responsibility. The Customer is the Controller.

5.3 Otherside has no control over the purpose and means of processing of the Personal Data. Otherside thus does not decide about the receipt and use of Personal Data, the disclosure to third parties, and the duration of storage of the personal data. Control over the personal data is never transferred to Otherside.

5.4 Besides Otherside's obligation to follow the Customer's instructions, Otherside must also ensure compliance with the conditions imposed on processing Personal Data, in particular under the GDPR.

5.5 Otherside must cooperate fully if the Supervisory Authority conducts audits, inspections, or investigations at the Customer in connection with this Supply Agreement.

5.6 Otherside must immediately inform the Customer in writing if the Dutch Data Protection Authority conducts audits, inspections, or investigations at Otherside (with the exception in case of a mandatory prohibition). Otherside must also inform the Customer of all findings of the Dutch Data Protection Authority that will have a direct or indirect effect on this Agreement.

5.7 Otherside must immediately follow the Dutch Data Protection Authority's recommendations relating to this Supply Agreement.

5.8 Otherside must forward a request for access, rectification, data portability, deletion of Personal Data, withdrawal of consent to process Personal Data or to restrict processing of Personal Data to the Customer (Data Subject's right) within five business days and cooperate fully with the Customer if such a request is made.

5.9 Otherside will cooperate in a Data Protection Impact Assessment (DPIA) at the Customer's request.

6 Security measures

6.1 Otherside must adopt all appropriate technical and organisational measures to secure the Personal Data against loss, destruction, or any form of unlawful processing. These measures must be appropriate, taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. These measures are at least aimed at:
1. Preventing unauthorised persons from gaining access to systems in which Personal Data are processed.
2. Preventing the use of systems in which Personal Data are processed without consent.
3. Ensuring that only authorised persons are allowed to Process the Personal Data in the relevant systems and that Personal Data cannot be Processed without the Customer's consent.
4. Ensuring that Personal Data cannot be read, copied, altered, or deleted without the Customer's consent during digital transfer or storage of the Personal Data.
5. Ensuring that it is possible to trace which Personal Data have been created, altered, or deleted in the systems in which they are processed and by whom.
6. Ensuring that Otherside's processors or subprocessors comply with all appropriate technical and organisational measures to secure the Personal Data against loss, destruction, or any form of unlawful processing.
7. Ensuring that Personal Data collected for different purposes can be processed separately.

6.2 In relation to the obligation described in the previous subparagraph, Otherside must at least adopt the measures specified in 'Privacy and Security Controls Otherside at Work'.

6.3 The measures that Otherside adopts in this regard must always comply with the ISO27001 system of standards, for which purpose a certifying body audits Otherside each year.

7 Accountability

7.1 Otherside must provide the Customer with the information that the Customer needs to form an opinion about Otherside's compliance with this Supply Agreement.
7.2 Immediately on request of the Customer, Otherside must explain the structure and operation of the system of measures and procedures aimed at ensuring compliance with this Supply Agreement.
7.3 During the term of this Supply Agreement, the Customer may examine the technical and organisational security measures that Otherside has adopted for their own Personal Data. The Customer may request all relevant IT security or privacy audit reports from Otherside for this purpose. The Customer may also conduct audits of Otherside's Personal Data processing operations. Otherside must provide the Customer with all information needed to conduct these audits.
7.4 On request, the Customer may conduct or have a security audit conducted on Otherside's relevant generic infrastructure, the client-specific infrastructure, and information security policy by qualified employees and/or third parties. An audit of the infrastructure and systems used for several customers is permitted, provided that these customers' interests are not harmed. Otherside will determine this in advance. Otherside and its processors and subprocessors must cooperate reasonably with the auditors acting on the Customer's behalf and give them access to the facilities where Personal Data are processed. This applies both to an audit of the infrastructure and/or information systems and to Otherside's offices and Colocation Data Centres. Otherside depends on the cooperation of the relevant service providers and/or suppliers at the Colocation Data Centres. If there is reason to do so, Otherside must commission a security audit itself.
7.5 The required cooperation by Otherside and/or its processors and subprocessors in an audit and the related costs will be charged to the Customer. Otherside provides all information that the Customer needs to carry out a data protection impact assessment itself, but passes on costs if the Customer needs support in developing the data protection impact assessment.

8 Employees and Subprocessors

8.1 If Otherside wishes to hire a third party ('subprocessor') to process the personal data, it will inform the Customer in advance. Otherside must ensure that all obligations under this Supply Agreement also apply to its processor and subprocessor.
8.2 The obligations imposed on Otherside under this Supply Agreement also apply to any party that processes the Personal Data under the authority of Otherside, the processor, or subprocessor.
8.3 Otherside must thus always oblige these persons, except in the case of mandatory legal obligations, to observe secrecy with regard to the Personal Data of which they become aware because of their relationship with Otherside.
8.4 The Customer authorises Otherside to involve hosting partner Proserve BV as a subprocessor at the Colocation Data Centres.

9 Data breaches

9.1 If a data breach as referred to in Article 33 GDPR, a security incident as referred to in Article 32 GDPR, or any other incident concerning the Personal Data occurs, Otherside must immediately, or at least within 24 hours after discovering the data breach, notify the Customer about this at the email address provided when this Supply Agreement was approved. Otherside warrants that the information provided will be complete, correct, and accurate insofar as the processor can reasonably determine at that time. Once additional relevant information about the data breach (or security breach) is known at a later stage, Otherside will inform Customer in more detail at the email address provided.
9.2 The notification obligation applies regardless of the scope and impact of the data breach.
9.3 Otherside's notification obligation towards the Customer always includes reporting that a data breach has occurred, as well as reporting:
- the actual or possible cause(s) of the data breach;
- the known and/or expected consequence(s) of the data breach;
- the confirmed or proposed solution(s);
- the contact details within Otherside's organisation for the follow-up of the report;
- the measures already taken to prevent recurrence.

10 Term, amendment and termination of the Agreement

10.1 The Supply Agreement is entered into from the moment the Data Safe is activated.
10.2 The Supply Agreement applies for an indefinite period.
10.3 If the Customer terminates the cooperation with its Service Provider and/or Service Provider terminates the cooperation with Otherside, this Supply Agreement will be terminated.
10.4 The Supply Agreement can be changed only in writing and with the Parties' consent.
10.5 If any article of this Supply Agreement is no longer valid or valid in its entirety because of a legislative or regulatory amendment, the Parties must consult with each other and agree on a replacement article that approximates the purport of the original article as closely as possible.
10.6 The parties have the right to terminate the Supply Agreement. This right must be exercised in writing.
10.7 As soon as, in accordance Article 10.3, the Customer terminates the cooperation with its Service Provider and/or Service Provider terminates the cooperation with Otherside, the Data Safe will be

deactivated. That is, all data in the Data Safe are destroyed and the Data Safe is no longer available.

10.8 Obligations arising from this Supply Agreement that continue by their nature after the termination of the Agreement will remain fully in force.

10.9 The Customer may terminate the Supply Agreement with immediate effect if Otherside does not comply with the obligations under this Supply Agreement.

10.10 Either Party may terminate the Supply Agreement with immediate effect if force majeure occurs. Force majeure also includes an amendment in the statutory rules to such an extent that continuing the Supply Agreement cannot reasonably be required.

10.11 As soon as the cooperation has ended, the Data Safe will be deactivated (in accordance with the explanation in Article 10.7), unless the Parties agree otherwise or if longer retention is required under laws or regulations or to be able to fulfil the obligations still arising from the cooperation. It is for the initiative of the Customer to make arrangements on this matter prior to terminating the cooperation with Otherside, including on receiving a written confirmation of the destruction of the Customer's Personal Data.

11 Liability

11.1 In addition to Article 6 of the Licence Terms, if a government regulator imposes a penalty on the Customer following an attributable breach by Otherside, or an act or omission that can be attributed to Otherside, and the penalty fully or partially relates directly to that breach, act, or omission, Otherside must indemnify the Customer against that penalty or the relevant part of it. The indemnity does not apply if the penalty relates, or also relates, to the Customer's own behaviour, or if the Customer could have reasonably taken measures to prevent the penalty. This indemnity is subject to the limitations on liability under the Licence Terms.