Verwerkersovereenkomst

Camas IT bv, gevestigd aan de Deventerweg 4d, 3843 GD Harderwijk, rechtsgeldig vertegenwoordigd door de heer J.A. Wijnholds, directeur, hierna te noemen: **(de) verwerker**

verklaren

te zijn overeengekomen een verwerkersovereenkomst als bedoeld in artikel 28 van de Algemene Verordening Gegevensbescherming.

Definities

1. De definities van de begrippen gebruikt in deze overeenkomst komen overeen met de definities in artikel 4 van de AVG. In aanvulling daarop gelden de volgende definities:
   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 en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming);
   Verwerkingsverantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt, in casu de opdrachtgever.
   Verwerker: degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtsreeks gezag te zijn onderworpen, in casu: Camas IT bv, gevestigd aan de Deventerweg 4D, 3843 GD Harderwijk.
   Betrokkene: degene op wie een persoonsgegeven betrekking heeft (in het kader van deze overeenkomst in ieder geval (ex-)werknemers).
   Autoriteit Persoonsgegevens: de toezichthouder als bedoeld in artikel 51 AVG.

Onderwerp van deze overeenkomst

2. In het kader van goed werkgeverschap wenst verwerkingsverantwoordelijke de gezondheid, competenties en motivatie van haar werknemers te bewaken en te bevorderen teneinde haar werknemers duurzaam inzetbaar te houden. Verwerkingsverantwoordelijke laat zich hierbij bijstaan door Perspectief Groep bv, hierna te noemen Perspectief, een gecertificeerde arbodienstverlener die zich richt op de duurzame inzetbaarheid van werknemers. Verwerkingsverantwoordelijke en Perspectief hebben hiertoe een overeenkomst (de hoofdovereenkomst) met elkaar gesloten en wensen hierbij gebruik te maken van het geautomatiseerde systeem CAMAS, geleverd door Camas IT bv.

3. Volgens de beleidsregels van de Autoriteit Persoonsgegevens mag Perspectief geen inzage hebben in de persoonsgegevens van niet-zieke werknemers. Naar aanleiding hiervan is in het geautomatiseerde systeem CAMAS sprake van:
   a) een werkgeversdeel van de verzuimregistratie, waarin de verwerkingsverantwoordelijke zijn deel van de verzuimregistratie kan voeren en waarin hij tevens alle personeelsgegevens kan invoeren,

zodat een compleet en actueel bestand van werknemers kan worden bijgehouden voor wie hij verantwoordelijk is ten aanzien van arbo- en verzuimverplichtingen, waarbij verwerkingsverantwoordelijke het doel en de middelen van de verwerking bepaalt, en
b) een gedeelte, inzichtelijk voor Perspectief, waarin (persoons)gegevens worden verwerkt van alleen die werknemers die zijn ziekgemeld door verwerkingsverantwoordelijke, zoals bedoeld in artikel 4 sub d van de hoofdovereenkomst, of zelf een beroep doen op de diensten van Perspectief.
CAMAS is hiermee enerzijds het verzuimsysteem voor verwerkingsverantwoordelijke, waarop deze verwerkersovereenkomst ziet, en anderzijds het systeem van Perspectief waarin deze als zelfstandige verwerkingsverantwoordelijke persoonsgegevens op basis van artikel 14 Arbeidsomstandighedenwet persoonsgegevens verwerkt voor het goed kunnen uitvoeren van de arbodienstverlening aan verwerkingsverantwoordelijke, zoals beschreven in de overeenkomst tussen Perspectief en verwerkingsverantwoordelijke (de hoofdovereenkomst), en waarvoor Perspectief met Camas IT een verwerkersovereenkomst heeft afgesloten.

Ingangsdatum en duur

4. De verwerkersovereenkomst gaat in op de datum van de hoofdovereenkomst waarvan deze verwerkersovereenkomst een bijlage is en wordt aangegaan voor de duur en eindigt op de datum van de hoofdovereenkomst. Wanneer de hoofdovereenkomst eindigt zonder dat partijen een nieuwe overeenkomst aangaan, eindigt de verwerkersovereenkomst van rechtswege. Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van de verwerkersovereenkomst voort te duren, blijven na beëindiging van de verwerkersovereenkomst gelden. Tot deze verplichtingen behoren onder meer die welke voortvloeien uit de bepalingen betreffende geheimhouding, overdracht en vernietiging, aansprakelijkheid en toepasselijk recht.

5. Indien Perspectief een andere dienstverlener (verwerker) dan Camas IT wenst te contracteren, dan zal verwerkingsverantwoordelijke per datum overgang eveneens naar de andere dienstverlener overgaan. Camas IT zal medewerking verlenen aan het overdragen van de (persoons)gegevens van verwerkingsverantwoordelijke aan deze andere dienstverlener, waarna deze verwerkersovereenkomst eindigt.

Naleving wet- en regelgeving

6. Verwerker verbindt zich de door verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens behoorlijk en zorgvuldig en in overeenstemming met de AVG en andere privacyregelgeving te verwerken, ingevolge deze verwerkersovereenkomst ten einde uitvoering te geven aan artikel 28 van de AVG.

7. Het is verwerker niet toegestaan de van verwerkingsverantwoordelijke verkregen persoonsgegevens voor doeleinden, anders dan overeengekomen, te verwerken of aan derden te verstrekken. Verwerkingsverantwoordelijke bepaalt het doel en de middelen voor de verwerking door verwerker.

8. Verwerkingsverantwoordelijke is verantwoordelijk voor de verwerkingen van persoonsgegevens zoals bedoeld in deze verwerkersovereenkomst. Verwerkingsverantwoordelijke verklaart persoonsgegevens te verwerken op een behoorlijke en zorgvuldige wijze en in overeenstemming

met de AVG en andere toepasselijke regelgeving betreffende de verwerking van persoonsgegevens. Verwerkingsverantwoordelijke verklaart aan verwerker dat de persoonsgegevens die verwerkt worden op basis van deze verwerkersovereenkomst, gezien de doeleinden waarvoor deze worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.

9. Verwerkingsverantwoordelijke treft de nodige maatregelen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn. Het is daarbij de verantwoordelijkheid van verwerkingsverantwoordelijke dat de persoonsgegevens in CAMAS doorlopend actueel, juist en volledig zijn, hetgeen betekent dat wijzigingen in persoonsgegevens, zoals mutaties van gegevens, direct moeten worden doorgevoerd. Verwerker is niet aansprakelijk voor het verwerken van onjuiste persoonsgegevens, indien blijkt dat deze door verwerkingsverantwoordelijke niet juist zijn ingevoerd. Verwerkingsverantwoordelijke is in een dergelijke situatie zelfstandig verantwoordelijk en aansprakelijk voor inbreuken op de beveiliging én melding daarvan aan de Autoriteit Persoonsgegevens en eventueel door haar opgelegde maatregelen.

10. Verwerker stelt verwerkingsverantwoordelijke in staat binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van betrokkenen zoals een verzoek om inzage, verbetering, aanvulling of verwijdering van gegevens én de verplichtingen in het geval van een inbreuk op de beveiliging.

11. In het geval dat een betrokkene een verzoek tot inzage, zoals bedoeld in artikel 15 AVG, of verbetering, aanvulling, wijziging of afscherming, zoals bedoeld in artikel 16 AVG e.v., aan de verwerkingsverantwoordelijke richt, dan zal verwerker meewerken aan het mogelijk maken van deze verzoeken. Verwerker mag de kosten voor de afhandeling doorbelasten aan verwerkingsverantwoordelijke.

Geheimhoudingsplicht

12. Verwerker is verplicht de van verwerkingsverantwoordelijke verkregen persoonsgegevens geheim te houden en haar betrokken personeelsleden en betrokken derden tot hetzelfde te verplichten, behoudens voor zover:

    - Verwerkingsverantwoordelijke de persoonsgegevens op grond van het bepaalde in artikel 3 van deze verwerkersovereenkomst via CAMAS aan Perspectief verstrekt.
    - Een wettelijk voorschrift verwerker tot mededelen verplicht.
    - De gegevensverstrekking plaatsvindt in opdracht van verwerkingsverantwoordelijke.
    - Het verstrekken van persoonsgegevens logischerwijze noodzakelijk is gezien de aard van de door verwerker verrichte dienstverlening aan verwerkingsverantwoordelijke.

13. Indien verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal verwerker verwerkingsverantwoordelijke, voorafgaand aan de verstrekking, ter zake informeren, tenzij wettelijke bepalingen dit verbieden.

14. De door of vanwege verwerker aan verwerkingsverantwoordelijke, of een instelling welke door verwerkingsverantwoordelijke is gemachtigd, verstrekte toegangs- of identificatiecodes en

certificaten zijn vertrouwelijk en zullen door verwerkingsverantwoordelijke en/of diens gemachtigden als zodanig worden behandeld en zullen slechts aan geautoriseerde medewerkers uit de organisatie van verwerkingsverantwoordelijke of de gemachtigde kenbaar worden gemaakt. Verwerker is gerechtigd toegewezen toegangs- of identificatiecodes en certificaten te wijzigen. Verwerker sluit elke aansprakelijkheid uit indien de verwerkingsverantwoordelijke of diens gemachtigde onzorgvuldig met verstrekte toegangs- of identificatiecodes omgaat.

Beveiligingsverplichtingen door verwerker

15. Verwerker garandeert passende organisatorische en technische maatregelen te nemen met betrekking tot de te verrichten verwerkingen van persoonsgegevens, tegen verlies of enige vorm van onrechtmatige verwerking, zoals onbevoegde kennisneming, aantasting, wijziging, verstrekking of verlies van de persoonsgegevens. Verwerker zal zich hierbij maximaal inspannen om de persoonsgegevens te beveiligen en beveiligd te houden tegen indringers en tegen van buiten komend onheil, alsmede onzorgvuldig, ondeskundig of ongeoorloofd gebruik. Verwerker is gecertificeerd voor ISO 27001 en NEN 7510 en garandeert hiervoor gecertificeerd te blijven. Verwerker heeft in ieder geval de maatregelen genomen zoals beschreven in bijlage 1.

16. Verwerker zal zijn beveiliging steeds aanpassen op grond van de stand der techniek en actuele inzichten in het beveiligen van persoonsgegevens. Het 'passend beveiligingsniveau' van artikel 28 en 32 AVG is hierbij het uitgangspunt.

17. In het geval van (vermoeden van) een inbreuk op de beveiliging zal de partij die dit constateert dit direct en onverwijld aan de andere partij melden, naar aanleiding waarvan de verwerkingsverantwoordelijke voor de gegevensverwerking in de gelegenheid is dit binnen de daarvoor gestelde termijnen van artikel 33 AVG aan de toezichthouder en eventueel de betrokkenen te melden. Partijen dragen zelf de kosten voor onderzoek naar de oorzaken van een inbreuk op de beveiliging. Het is ter uitsluitende beoordeling van de verwerkingsverantwoordelijke om te bepalen of een inbreuk op de beveiliging een meldingsplichtige inbreuk betreft in de zin van de AVG.

18. De meldplicht als bedoeld in artikel 17 behelst in ieder geval het melden van het feit dat er een inbreuk op de beveiliging is geweest, alsmede het exacte tijdstip van deze inbreuk, het systeem en feiten van het voorval, de (vermeende) oorzaak van de inbreuk, de te verwachten gevolgen van de inbreuk voor betrokkenen alsmede de voorgestelde oplossing. Tevens dienen vermeld te worden de getroffen maatregelen om de schade te beperken en de inbreuk te repareren, de getroffen maatregelen om herhaling te voorkomen alsmede de maatregelen om de negatieve gevolgen zoveel als mogelijk direct te beperken, waaronder begrepen communicatie aan derden en betrokkenen.

19. Het is verwerker alleen toegestaan de persoonsgegevens van verwerkingsverantwoordelijke op te slaan op gegevensdragers welke zijn gelokaliseerd in de EU/EER, dan wel binnen een land, waarvan de Europese Commissie heeft verklaard dat het beveiligingsniveau adequaat is.

20. Het is verwerkingsverantwoordelijke toegestaan proces en inhoudelijke audits uit te (laten) voeren op de verwerkingen die verwerker doet in het kader van het bepaalde in deze overeenkomst. Verwerker zal alle medewerking verlenen om dergelijke audits mogelijk te maken, waarbij

personeel van de auditer toegang krijgt tot documentatie, handleidingen en de systemen. Verwerkingsverantwoordelijke, of de door verwerkingsverantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze audits vertrouwelijk te behandelen. Kosten voor een dergelijke audit komen voor rekening van verwerkingsverantwoordelijke.

Inschakeling derden

21. Het is verwerker toegestaan een subverwerker in te schakelen voor zover dit noodzakelijk is voor het uitvoeren van de werkzaamheden uit deze overeenkomst. De verwerker blijft verantwoordelijk voor deze subverwerker(s) en zal minimaal dezelfde eisen aan deze subverwerker(s) opleggen op het gebied van passende technische en organisatorische maatregelen als in deze verwerkersovereenkomst is opgenomen.

22. Verwerkingsverantwoordelijke geeft toestemming voor het inschakelen van de subverwerkers die verwerker op moment van aangaan van deze overeenkomst heeft ingeschakeld. Dit betreft Microsoft Ireland Operations Limited, statutair gevestigd in Dublin, voor Microsoft Cloud Services waaronder Microsoft Azure met als doel het doen van statistische analyses op grond van artikel 89 AVG.

Wijziging overeenkomst

23. Wanneer de AVG dan wel de van toepassing zijnde richtsnoeren van de Autoriteit Persoonsgegevens wijzigen of andere relevante regelgeving van kracht wordt, treden partijen in overleg om te bezien of en hoe deze verwerkersovereenkomst moet worden gewijzigd.

24. Verwerker draagt er zorg voor dat persoonsgegevens onverwijld na de beëindiging van deze overeenkomst, of zoveel eerder als dat mogelijk is, nadat deze gegevens voor zover noodzakelijk zijn overgedragen aan verwerkingsverantwoordelijke, vernietigd worden, tenzij een bewaartermijn van toepassing is. Verwerker toont op eerste verzoek van Verwerkingsverantwoordelijke aan dat dit daadwerkelijk is gebeurd.

Bewaartermijnen

25. Verwerker bewaart de persoonsgegevens niet langer dan strikt noodzakelijk en in geen geval langer dan tot het einde van deze overeenkomst of, indien tussen partijen een bewaartermijn van toepassing is of is overeengekomen, niet langer dan deze termijn.

26. Camas IT heeft vanuit het oogpunt Privacy by design de mogelijkheid gecreëerd om de verschillende vastgestelde bewaartermijnen voor medische gegevens, gezondheidsgegevens en overige persoonsgegevens automatisch toe te passen op de verzuimdossiers in CAMAS. Op basis van Privacy by default staat deze instelling standaard aangevinkt. De verwerkingsverantwoordelijke kan deze instelling per werknemer uitvinken. Na afloop van de bewaartermijn worden de gegevens op dossierniveau verwijderd. Voor analytische doeleinden

worden bepaalde geanonimiseerde gegevens bewaard. Om de beschikbaarheid te garanderen worden back ups vier weken bewaard. Daarna blijft de back up van elke eerste dag van de maand bewaard, welke na een jaar wordt vernietigd.

Aansprakelijkheid

27. Een partij is aansprakelijk voor directe schade voortvloeiende uit het niet-nakomen van of in strijd handelen met de bij of krachtens de AVG gegeven voorschriften en/of het niet-nakomen van of in strijd handelen met de in deze verwerkersovereenkomst opgenomen bepalingen, of uit aansprakelijkheid voor onrechtmatige daad. Aansprakelijkheid voor gevolgschade is uitgesloten. Onder gevolgschade wordt gerekend gederfde winst, gemiste inkomsten, boetes en reputatieschade. De aansprakelijkheid is voorts beperkt tot het bedrag dat door de aansprakelijkheidsverzekering van Verwerker wordt gedekt en ter zake daadwerkelijk door haar verzekeraar wordt uitgekeerd.

Toepasselijk recht

28. Op deze verwerkersovereenkomst is uitsluitend Nederlands recht van toepassing.

Bijlage 1

Beveiligingsmaatregelen:

1. Een passend en uitgeschreven (informatie)beveiligingsbeleid, waarbij het vermogen wordt gegarandeerd om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te borgen.

2. Encryptie (versleuteling) van digitale bestanden met medische persoonsgegevens.

3. Two factor authentication.

4. Beveiliging van netwerkverbindingen via Secure Socket Layer (SSL) technologie.

5. Het installeren en werken met de meest actuele virusscanners om data te beschermen tegen onder andere malware.

6. Periodiek een back up maken van de (persoons)gegevens, zodat verlies van data is uitgesloten. Back ups worden versleuteld opgeslagen.

7. Actief monitoren op inbreuken op de beveiligingsmaatregelen.

8. Afsluitbare kasten en ruimten met toegangsbeveiliging voor plaatsen waar de persoonsgegevens van verwerkingsverantwoordelijke zijn opgeslagen.

9. Het frequent evalueren en verbeteren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking conform de ontwikkeling van de techniek.

10. Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot persoonsgegevens tijdig te herstellen.