INTERN PRIVACYBELEID

VOOR DE VERWERKING VAN PERSOONSGEGEVENS

Versie 2.0 – juli 2019

adding PRAKTIJK VOOR TANDHEELKUNDE

1. INTRODUCTIE

Dit is het privacybeleid (hierna: het "Privacybeleid") van Adding, Praktijk voor Tandheelkunde (hierna: de "Praktijk"). Dit privacybeleid ziet zowel op het verzamelen en verwerken van persoonsgegevens die in verband met de hulp- en zorgverlening aan patiënten worden verwerkt, als op gegevens van medewerkers die binnen de Praktijk worden gebruikt. Het privacybeleid beschrijft op welke wijze de Praktijk met deze gegevens omgaat en welke protocollen en processen zij binnen de Praktijk heeft geïmplementeerd om ervoor te zorgen dat de veiligheid van de gegevens gewaarborgd is en dat aan de vereisten van de Algemene verordening gegevensbescherming ("AVG") wordt voldaan.

In dit privacybeleid komen de volgende onderwerpen aan bod.

- Verwerkingsregister
- Type persoonsgegevens en doelen
- Informatieplicht
- Rechten van betrokkenen
- Derde partijen
- Beveiliging
- Datalekken
- Bewaartermijnen
- Privacy Impact Assessment
- Doorgifte van persoonsgegevens
- FG

De protocollen en overige documenten waarnaar in dit Privacybeleid wordt verwezen, zijn als bijlage aan het Privacybeleid gehecht.

Om ervoor te zorgen dat dit Privacybeleid blijft aansluiten bij de verwerking van persoonsgegevens binnen de Praktijk, zal het Privacybeleid jaarlijks worden geëvalueerd. Aan de hand van die evaluatie zal, indien vereist, het Privacybeleid en de hieraan gehechte protocollen en documenten worden aangepast. Indien op een moment voor de evaluatie duidelijk wordt dat het Privacybeleid aanpassing behoeft, zal de Praktijk de vereiste aanpassingen op dat moment al doorvoeren.

Verwerkingsverantwoordelijke
degene die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Dat is dus de partij die bepaalt wat er met de gegevens gebeurt. De Praktijk is als verwerkingsverantwoordelijke aan te merken.

Verwerker
een partij die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Deze partij bepaalt dus **niet** voor welk doel gegevens worden verzameld en gebruikt. Voorbeelden zijn de partijen die het salarisadministratiesysteem en het patiëntsysteem aanbieden.

Persoonsgegevens
Alle informatie direct of indirect tot een persoon te herleiden is. Hieronder vallen naast de NAW-gegevens ook alle andere patiënt- en behandelgegevens, zoals gebitsfoto's.

2. PRIVACYBELEID

2.1. Verwerkingsregister

De Praktijk houdt een verwerkingsregister bij. Dit register bevat onder meer een beschrijving van de (categorieën) persoonsgegevens die binnen de Praktijk worden verwerkt, de doelen waarvoor ze worden verwerkt, de derden aan wie de

gegevens worden verstrekt, de bewaartermijn van de gegevens en de technische en organisatorische maatregelen die zijn genomen om de gegevens te beschermen.

In het verwerkingsregister dient voor elke verwerking opgenomen te worden welke persoonsgegevens worden verzameld en voor welk doel ze worden gebruikt. Voorbeelden van gegevensverwerkingen zijn:

- Het vastleggen en bijhouden van persoonsgegevens van een patiënt in het kader van de behandeling van de patiënt;
- het gebruiken van persoonsgegevens ten behoeve van facturatie;
- het verstrekken van (medische) gegevens aan een derde, bijvoorbeeld ten behoeve van een doorverwijzing;
- het vastleggen van persoonsgegevens voor het aanleggen en bijhouden van een medisch dossier; of
- het registreren van persoonsgegevens in een systeem om een nieuwe patiënt in te schrijven.

Binnen de Praktijk heeft/hebben Géke Lassche en Nynke Adding, praktijkmanagers toegang tot het register. Gerda Olijve en Diana de Meijere, baliemedewerkers hebben alleen de mogelijkheid het register te raadplegen. Tinka van Lieren Nynke Adding, praktijkmanagers kunnen het register raadplegen en daar wijzigingen in aanbrengen.

Het register wordt door de Praktijk continue en actief bijgehouden. Wijzigingen in de verwerking van persoonsgegevens worden direct in het register doorgevoerd. Tijdens de kwartaalevaluatie zal ook worden beoordeeld of het register nog altijd accuraat is of dat aanpassingen in het register vereist zijn.

2.2. Type persoonsgegevens en doeleinden

Binnen de Praktijk worden persoonsgegevens van twee categorieën personen verwerkt: i) de patiënten en ii) de medewerkers.

Patiënten

Indien een patiënt zich aanmeldt aan de balie binnen de Praktijk, worden allereerst de persoonsgegevens vereist voor inschrijving verstrekt. In aanvulling hierop wordt een gezondheidsformulier verstrekt dat door de patiënt moet worden ingevuld. Op dit formulier worden vragen gesteld omtrent de gezondheid van de patiënt die van belang kunnen zijn voor de behandeling.

Indien een patiënt zich telefonisch of via de website van de Praktijk aanmeldt, wordt de patiënt verzocht de gegevens te verstrekken die vereist zijn voor registratie. Het gezondheidsformulier wordt niet via de website verstrekt en telefonisch worden de vragen op het gezondheidsformulier niet uitgevraagd.

Indien de patiënt afkomstig is van een andere praktijk, kunnen persoonsgegevens van die andere praktijk worden verkregen. De patiënt kan de gegevens zelf meenemen, maar deze kunnen ook per reguliere post of per e-mail via het beveiligde zorgmail aan de Praktijk worden toegezonden.

Alle gegevens die de Praktijk verkrijgt in het kader van het inschrijven van een patiënt, worden (gescand) opgeslagen in Simplex (hierna: het "Systeem").

Naast de gegevens vereist voor inschrijving bij de Praktijk, verwerkt de Praktijk gegevens die verband houden met de behandeling van de patiënt. Het gaat daarbij onder meer om afspraken, gegevens omtrent de uitgevoerde handelingen, gemaakte foto's, kronen en verwijzingen naar andere zorgverleners. Al deze gegevens worden tevens in het Systeem opgeslagen.

In het Systeem worden ook de facturen voor de patiënten aangemaakt. De Praktijk verzendt de facturen vervolgens naar een factoringmaatschappij of incassobureau die het innen van de facturen bij de patiënt of de verzekeraar verzorgt.

Alle gegevens die over de patiënt worden verzameld, worden gebruikt met als doel de hulp- en zorgverlening voor de patiënt.

Bij intercollegiale toetsing binnen een praktijk of instelling kunnen gegevens worden gebruikt en verstrekt. De patiënt wordt daarvan tevoren van op de hoogte gebracht.

Veilig Incident Melden (VIM)

Binnen de praktijk is Tinka van Lier, praktijkmanager, degene die zorgdraagt voor de procedure om incidenten te melden, zich inzet voor een cultuur binnen de praktijk dat incidenten worden gemeld en die ervoor zorgt dat meldingen worden geanalyseerd ("de Functionaris").

Meldingen van incidenten kunnen op papier worden gedaan. De melding bevat zowel persoonsgegevens van de betreffende medewerker van de Praktijk als de patiënt in kwestie.

De Functionaris brengt de meldingen in voor nadere oorzakenanalyse in de analysegroep. De analysegroep analyseert vervolgens de melding en behandelt deze vertrouwelijk. Indien nodig vraagt de analysegroep nadere informatie aan de melder.

Van het incident wordt aantekening gemaakt in het patiëntendossier van de patiënt, waarin wordt vermeld: de aard en toedracht van het incident; het tijdstip waarop het incident heeft plaatsgevonden; en de namen van de bij het incident betrokken zorgverleners.

De Praktijk zorgt dat meldingen vertrouwelijk worden behandeld en dat de meldingen zo worden bewaard dat deze niet toegankelijk zijn voor anderen.

Toezicht en handhaving

Op grond van de Wkkgz maakt de Praktijk bij de IGZ melding van eventuele calamiteiten die bij de zorgverlening hebben plaatsgevonden. Ook meldt de Praktijk het bij de IGZ als er geweld bij de zorgverlening heeft plaatsgevonden of als de arbeidsrelatie met een individuele zorgverlener is beëindigd vanwege ernstige functioneringsproblemen.

Op grond van de wet komt aan de IGZ een aantal bevoegdheden toe bij het houden van toezicht op specifieke volksgezondheidswetten. Bij onderzoek dat specifiek is gericht op individuele casuïstiek, heeft de IGZ recht op inzage in medische dossiers voor zover deze inzage nodig is voor de uitvoering van haar taken. De Praktijk is dan gehouden om de IGZ inzage te verlenen.

De Nederlandse Zorgautoriteit (NZa) is onder meer belast met markttoezicht, marktontwikkelingen, tarief- en prestatieregulering en met toezicht op de uitvoering van de Zorgverzekeringswet en de Wet langdurige zorg (Wlz). In dat kader kan de Praktijk in sommige gevallen verplicht zijn om op verzoek bepaalde gegevens aan de NZa te verstrekken. Het kan hier gaan om identificerende gegevens die hemzelf betreffen, om andere identificerende persoonsgegevens en om medische persoonsgegevens van patiënten.

Medewerkers

In het kader van de uitvoering van de arbeidsovereenkomst, verwerkt de Praktijk ook persoonsgegevens van haar medewerkers. De arbeidsovereenkomst en daarmee samenhangende gegevens worden opgeslagen in het schriftelijke personeelsdossier wat achter een gesloten deur wordt beveiligd.. Deze gegevens worden in eerste instantie gebruikt voor het vaststellen en uitbetalen van het salaris van de medewerkers. Welke uitgevoerd wordt door RDW (Rooker en De Wit)

In het personeelsdossier kunnen ook gegevens omtrent eventuele klachten, waarschuwingen, beoordelingen en verzuimfrequentie worden opgeslagen. Voor zover aan medewerkers een mobiele telefoon, leaseauto, laptop en/of toegangspas ter beschikking wordt gesteld, wordt dit voor administratieve doeleinden geregistreerd.

De toegang tot de personeelsdossiers is beveiligd. Binnen de Praktijk heeft Géke Lassche, praktijkmanager en Nynke Adding, praktijkmanager, toegang tot het personeelsdossier.

De Praktijk is wettelijk gehouden bepaalde persoonsgegevens van medewerkers aan derde partijen te verstrekken. Deze verstrekking aan derde partijen heeft de volgende doeleinden:

- Bij indiensttreding wordt aan de collectieve zorgverzekeraars en andere collectieve verzekeraars de datum van indiensttreding, NAW-gegevens en het BSN van medewerkers doorgegeven.
- Ziek- en herstelmeldingen worden doorgegeven aan de Arbodienst.
- Bij uitdiensttreding vanwege ziekte en bij zwangerschapsverlof worden gegevens van medewerkers aan het UWV doorgegeven in verband met het verkrijgen van een vangnetuitkering, waaronder salaris, pensioenpremie, prepensioen, hiaatverzekering, de NAW-gegevens en het BSN.
- Aan pensioenfondsen en andere daaraan gelieerde instellingen en organisaties worden eveneens gegevens verstrekt.

Gegevens omtrent het functioneren van medewerkers worden ook verwerkt in het kader van individuele kwaliteitsverbetering. De verzamelde gegevens worden dan gebruikt voor het coachen en trainen van medewerkers met het doel hen beter te laten functioneren.

Gegevens omtrent het functioneren van medewerkers kunnen ook gebruikt worden voor de beoordeling van de medewerker, bijvoorbeeld in het kader van functioneringsgesprekken. De gegevens die de Praktijk verzamelt om medewerkers te beoordelen, kunnen door de medewerkers worden ingezien waarbij de medewerker kans krijgt om hierop te reageren. De verslaglegging van functioneringsgesprekken dient als uitgangspunt bij een volgend gesprek en wordt benut als managementinformatie.

Tot slot kan het zo zijn dat, in het kader van het verbeteren van de bedrijfsprocessen, binnen de Praktijk, persoonsgegevens van medewerkers worden verwerkt.

Deze categorieën van persoonsgegevens, van zowel de patiënten als de medewerkers, staan vermeld in het verwerkingsregister.

ZZP'ers

In het kader van de uitvoering van een overeenkomst van opdracht met een ZZP'er, verwerkt de Praktijk ook persoonsgegevens van ingeschakelde ZZP'ers. De overeenkomst van opdracht en daarmee samenhangende gegevens worden opgeslagen in het personeelsdossier achter een gesloten deur. De Praktijk vraagt de ZZP'ers niet om een kopie of scan van hun identiteitsbewijs te verstrekken.

Tot 1 mei 2016 moest een ZZP'er een kopie of scan van zijn identiteitsbewijs afstaan aan de opdrachtgever als de ZZP'er een Verklaring arbeidsrelatie (VAR) gebruikte. Door de invoering van de Wet deregulering beoordeling arbeidsrelaties (DBA) is dat nu niet meer verplicht. De VAR is per 1 mei 2016 vervallen. Opdrachtgevers en zzp'ers of freelancers kunnen nu – als zij dat willen – een modelovereenkomst gebruiken. Indien met zo'n modelovereenkomst wordt gewerkt, dan is het zeker dat de opdrachtgever geen loonheffingen hoeft in te houden.

2.3. Informatieplicht

De Praktijk stelt de patiënten bij inschrijving op de hoogte van de persoonsgegevens die zij over de patiënt verzamelt en voor welke doeleinden deze persoonsgegevens vervolgens worden gebruikt.

Bij de inschrijving aan de balie in de Praktijk wordt bij de inschrijving en/of het gezondheidsformulier het privacy statement van de Praktijk aan de patiënt verstrekt. Bij een inschrijving via de website wordt tijdens het proces van inschrijving door middel van een hyperlink verwezen naar het privacy statement. Bij een telefonische inschrijving wordt de patiënt verteld dat zijn gegevens worden gebruikt voor inschrijving. Vervolgens wordt bij het invullen van het gezondheidsformulier het privacy statement verstrekt. Het privacy statement is als Bijlage 1 aan dit Privacybeleid gehecht.

Bij indiensttreding wordt aan de medewerkers kenbaar gemaakt voor welke doeleinden hun persoonsgegevens worden verwerkt en wat er van hun in het kader van privacy mag worden verwacht.

Werknemers privacybeleid
De verwerking van persoonsgegevens van werknemers, is aan dezelfde privacyregels onderworpen als de gegevensverwerking van andere betrokkenen, zoals patiënten. Evenals patiënten hebben werknemers daarom het recht om geïnformeerd te worden over de vastlegging van hun persoonsgegevens, al dan niet in het personeelsdossier en het gebruik van die gegevens. Informatie over waarom gegevens van werknemers worden verzameld, kan worden opgenomen in een werknemers privacybeleid dat voorafgaand aan de ondertekening van de arbeidsovereenkomst aan de werknemer wordt verstrekt.

2.4. Rechten van betrokkenen

Alle verzoeken, op welke wijze ook binnengekomen (telefonisch, per e-mail, per brief), van een patiënt of medewerker waarin rechten ten aanzien van persoonsgegevens worden ingeroepen, worden verzonden aan Tinka van Lier, praktijkmanager, via info@adding.nl. Verzoeken en alle overige afhandeling worden opgeslagen in de map Verbeterformulieren.

Na ontvangst van een verzoek zal de Praktijk eerst de identiteit van de verzoeker verifiëren. De Praktijk kan de verzoeker vragen een kopie van een identiteitskaart mee te zenden. De Praktijk zal daarbij aan de verzoeker aangegeven dat het BSN niet mag worden verstrekt en dus van de kopie van de identiteitskaart verwijderd moet worden.

Indien de identiteit van de betrokkene is vastgesteld, zal de Praktijk de verzoeker laten weten dat er binnen één maand op het verzoek zal worden gereageerd. Indien het verzoek complex is, kan deze termijn met maximaal twee maanden worden verlengd. Indien dit het geval is, zal de Praktijk dit binnen de initiële maand aan de verzoeker laten weten.

Géke Lassche, praktijkmanager zal vervolgens vaststellen welk recht precies wordt ingeroepen en verzamelt de in dat kader vereiste informatie. Op basis van deze informatie wordt een verslag opgesteld. Of dit verslag wordt besproken met juridische ondersteuning. Op basis van dit verslag wordt besloten of, en zo ja, op welke wijze aan het verzoek van de verzoeker kan worden voldaan.

Voor de communicatie richting de verzoeker en het treffen van maatregelen naar aanleiding van een verzoek zullen in beginsel geen kosten in rekening worden gebracht bij de verzoeker. Slechts in bepaalde gevallen zal de Praktijk kosten in rekening brengen (een redelijke vergoeding in het licht van de administratieve kosten). Bijvoorbeeld wanneer verzoeker meerdere inzageverzoeken of herhaaldelijk ongegronde verzoeken indient. De Praktijk mag in uitzonderingsgevallen ook weigeren om gevolg te geven aan het verzoek.

Indien gevolg wordt gegeven aan het verzoek van een verzoeker, dienen in bepaalde gevallen ook derde partijen op de hoogte te worden gesteld. Het verslag dient daarom ook de derde partijen te beschrijven die betrokken zijn bij het honoreren van een verzoek van de verzoeker. Dergelijke kennisgevingen laat de Praktijk achterwege als dit onmogelijk blijkt of onevenredig veel inspanning vergt.

De Praktijk heeft zodanige technische maatregelen genomen dat aan verzoeken van verzoekers kan worden voldaan. Zo kan de Praktijk een verzoeker inzage verlenen in de gegevens die over hem/haar worden verzameld, kunnen gegevens worden verwijderd of verbeterd, kan de verwerking van gegevens tijdelijk worden gestaakt, kunnen deze gegevens makkelijk overgezet worden naar een nieuwe aanbieder en wordt er bij de intrekking van toestemming zorg voor gedragen dat de gegevens vanaf dat moment niet weer voor dat doel worden gebruikt.

2.5. Derde partijen

De Praktijk maakt voor het verwerken van persoonsgegevens gebruik van derde partijen. Het gaat daarbij onder meer om partijen die louter ten behoeve van de Praktijk gegevens verwerken (hierna: "Verwerkers").

Met deze Verwerkers heeft de Praktijk een verwerkersovereenkomst afgesloten waarin onder meer de mate van beveiliging van de persoonsgegevens die de Verwerker voor de Praktijk verwerkt wordt beschreven. Ook bevat de verwerkersovereenkomst bepalingen omtrent het uitvoeren van een audit bij de Verwerker en de procedure die moet worden gevolgd als van een incident omtrent persoonsgegevens sprake is. De standaard-verwerkersovereenkomst die de Praktijk hanteert, is als Bijlage 2 aan dit privacybeleid gehecht.

In de Praktijk wordt van de volgende Verwerkers gebruik gemaakt Supracom BV, partij die onderhoud doet voor Windows en Exquise.

- W3apponline, in het kader van hosting en onderhoud aan de webagenda
- Studio Eijsink, in het kader van hosting en onderhoud van de website
- GSN in het kader van automatisering en onderhoud en support van tandheelkundige software Simplex
- VECOZO voor controle van patiëntgegevens bij de zorgverzekeraar en/of het verzenden van gegevens aan zorgverzekeraar
- Factoringmaatschappij Infomedics voor de facturatie en inning van facturen
- Zorgmail in het kader van de verzending van gegevens
- RDW in het kader van het vaststellen en uitbetalen van het salaris
- Cerec in het kader van onderhoud en support (op afstand)
- Yvonne's Tandtechniek in het kader van het produceren van onder meer kronen
- Orthodontisch Laboratorium Friesland in het kader van het produceren van orthodontische apparatuur.
- Sentix, in het kader van onderhoud/support van röntgenapparatuur
- Arseus Dental, voor VisieQuick in het kader van hosting en/of onderhoud en support van röntgenapparatuur
- Roozeboom, alleen mailadressen, in het kader van de isocertificering

Persoonsgegevens van patiënten of medewerkers worden aan andere verwerkingsverantwoordelijken doorgegeven wanneer dat wettelijke vereist is, noodzakelijk is in het kader van hulp- en zorgverlening van de patiënt (verwijzingen) en voor intercollegiaal overleg. Buiten deze situatie worden persoonsgegevens niet aan andere verwerkingsverantwoordelijken verstrekt zonder voorafgaande uitdrukkelijke toestemming van de patiënt of medewerker. Dat is alleen anders indien er een wettelijke verplichting tot verstrekking bestaat of indien de gegevens in het verlengde van de zorg- en hulpverlening gedeeld moeten worden, bijvoorbeeld in het kader van intercollegiaal overleg. Daarbij geldt dat alleen de strikt noodzakelijk geachte gegevens worden verstrekt.

2.6. Beveiliging

De Praktijk hecht veel waarde aan de beveiliging van zowel de patiëntgegevens als de gegevens van haar medewerkers. De Praktijk heeft daarom passende technische en organisatorische maatregelen genomen om deze persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.

Voor zover de Praktijk gebruikmaakt van Verwerkers zijn met deze Verwerkers afspraken gemaakt over de te nemen technische en organisatorische maatregelen. Hierbij wordt een risicoanalyse gemaakt. Op grond van de risico's die de persoonsgegevens en de aard van de verwerking met zich meebrengen, wordt het gewenste beveiligingsniveau bepaald.

De Praktijk heeft op grond van de verwerkersovereenkomst het recht de door de Verwerker getroffen maatregelen periodiek te auditen, testen, beoordelen en evalueren om zo te bepalen of de overeengekomen maatregelen worden nageleefd en of deze nog doeltreffend zijn en om deze zo nodig aan te laten passen.

De Praktijk hanteert in aanvulling op het bovenstaande ook interne beveiligingsmaatregelen. Het gaat daarbij onder meer om de volgende maatregelen:

- Persoonsgegevens worden op een beveiligde wijze uitgewisseld en niet via WhatsApp, Dropbox of Gmail
- Persoonsgegevens worden niet op USB sticks of andere mobiele dragers gekopieerd tenzij de persoonsgegevens versleuteld worden
- Alleen Gerda Olijve, Ingrid Hoekstra, Martine Faber, Diana de Meijere, Yvette Koedijk, Ineke Mulder, baliemedewerkers, Géke Lassche en Nynke Adding, praktijkmanagers, Wout Vochteloo, Rob Adding en Chantal Schreuder, tandartsen, hebben toegang tot de patiëntgegevens
- Alleen Géke Lassche en Nynke Adding, praktijkmanagers, hebben toegang tot personeelsdossiers
- Wachtwoorden zijn voldoende sterk en worden periodiek vervangen
- Toegang tot het Systeem op afstand is alleen mogelijk via een beveiligde VPN verbinding op basis van twee-staps authenticatie
- Binnen de Praktijk zijn processen ingericht die aangeven wat er moet gebeuren indien een incident inzake persoonsgegevens zich voordoet of indien patiënten of medewerkers een beroep op hun rechten doen
- Devices als laptops en mobiele telefoons worden niet onbeheerd achtergelaten, worden versleuteld opgeslagen en verlies/diefstal dient direct te worden gemeld bij de praktijkmanager
- Het is medewerkers niet toegestaan, zonder toestemming van de praktijk, software te downloaden en/of om firewalls of virusscanner aan te passen of te verwijderen
- Toegang tot het pand is alleen mogelijk met aan medewerkers verstrekte sleutels
- Teneinde de veiligheid van patiënten en medewerkers te garanderen is er zichtbaar een camera geplaatst in de praktijk. Aan de hand van deze camera kan, op afstand, in de gaten gehouden worden of er zich onveilige of niet gewenste situaties voordoen. Tevens kan middels deze camera diefstal worden gesignaleerd.

Binnen de Praktijk worden elke dag back-ups gemaakt. Hiermee realiseert de Praktijk dat in het geval van een incident met persoonsgegevens (bijvoorbeeld in het geval van ransomware) een recente back-up teruggezet kan worden zodat persoonsgegevens niet blijvend verloren gaan.

De interne beveiligingsmaatregelen kunnen door de Praktijk steekproefsgewijs worden gecontroleerd. Controle zal altijd zo kort en zo beperkt mogelijk uitgevoerd worden. Indien er een gerichte verdenking bestaat tegen een medewerker kan tot gerichte controle worden overgegaan. Aan de hand van de uitkomst van steekproeven kunnen door de Praktijk disciplinaire maatregelen genomen worden.

Uitgangspunt binnen de Praktijk is dat niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken waarvoor ze zijn verzameld. Zo vraagt de Praktijk niet meer informatie uit bij de patiënt dan noodzakelijk is voor zorg- en hulpverlening. Ook bij het inschakelen van derde partijen, beoordeelt de Praktijk of de door die derde partij aangeboden dienst aansluit bij het doel dat de Praktijk voor ogen heeft en er niet meer persoonsgegevens worden verzameld dan daarvoor nodig is (*privacy by design en privacy by default*).

2.7. Datalekken

De Praktijk heeft passende technische en organisatorische maatregelen genomen die tot doel hebben de kans op verlies of onrechtmatige verwerking van persoonsgegevens zo veel mogelijk te beperken. Ondanks deze maatregelen bestaat de kans dat zich toch een incident met betrekking tot persoonsgegevens voordoet. Om ervoor te zorgen dat er zo snel mogelijk opgetreden kan worden om het incident te beëindigen en de schade zo veel mogelijk te beperken, heeft de Praktijk een incident response protocol opgesteld. De Praktijk maakt eveneens gebruik van een stappenplan datalek melden en het document datalek melden of niet van de KNMT, welke als Bijlage X bij dit privacybeleid zijn gevoegd.

Elk incident met betrekking tot persoonsgegevens moet worden gemeld aan Géke Lassche, praktijkmanager via geke@tandartspraktijkadding.nl. Géke Lassche, praktijkmanager zal vervolgens bepalen of:

- er inderdaad sprake is van een incident dat betrekking heeft op persoonsgegevens
- welke maatregelen genomen moeten worden om het incident te stoppen en de gevolgen te beperken
- er een externe partij moet worden ingeschakeld om bij de oplossing van het incident te assisteren
- het incident aan de Autoriteit Persoonsgegevens moet worden gemeld. De melding aan de Autoriteit Persoonsgegevens zal vervolgens binnen 72 uur nadat de Praktijk op de hoogte is geraakt van het incident plaatsvinden
- degenen op wie de persoonsgegevens betrekking hebben, moeten worden geïnformeerd over het incident
- welke maatregelen er genomen moeten worden om herhaling van het incident te voorkomen

Voor het geval ook betrokkenen geïnformeerd moeten worden over een incident, hanteert de Praktijk een standaardbrief welke als Bijlage 3 bij dit privacybeleid is gevoegd.

Aangezien de kans bestaat dat een Verwerker als eerste op de hoogte raakt van een (potentieel) incident, is in de Verwerkersovereenkomst afgesproken dat de Verwerker de Praktijk zo snel mogelijk op de hoogte stelt van een incident. Ook zijn er afspraken gemaakt over het oplossen van het incident en het verstrekken van nadere gegevens.

De Praktijk documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Dit logboek wordt opgeslagen in Word op schijf J in een met wachtwoord beveiligde map 'Adding> AVG logboek

2.8. Bewaartermijnen

De Praktijk hanteert een beleid voor het bewaren van persoonsgegevens. Persoonsgegevens die niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verzameld en tevens niet op grond van andere wetgeving bewaard moeten worden, worden door de Praktijk verwijderd. De persoonsgegevens dienen in dat geval ook uit eventuele back-ups, archieven en andere systemen te worden verwijderd.

Patiëntgegevens

Patiëntgegevens worden op grond van de bewaarplicht van medische behandelgegevens bewaard gedurende een periode van vijftien (15) jaar.

Gegevens medewerkers

De Praktijk bewaart gegevens van medewerkers voor zover vereist op basis van fiscale boekhoud- en administratieplicht gedurende een periode van 7 jaar.

Voor zover de betreffende gegevens niet vallen onder de fiscale boekhoud- en administratieplicht, hanteert de Praktijk de volgende bewaartermijnen:

- Loonadministratie (gedurende 5 jaar)
- Loonbelastingverklaring (gedurende 5 jaar na uitdiensttreding)
- Kopie identiteitsbewijs werknemer (gedurende 5 jaar na uitdiensttreding)

Overige persoonsgegevens

Gegevens die met behulp van camerabeelden worden verzameld, worden gedurende vier (4) weken bewaard tenzij langer bewaren noodzakelijk is in verband met geconstateerde strafbare feiten.

Ten aanzien van facturen die niet als medische behandelgegevens kwalificeren, bijvoorbeeld facturen aan/van derde partijen, bewaart de Praktijk deze in verband met de omzetbelasting gedurende een periode van zeven (7) jaar.

2.9. Doorgifte buiten EER

De Praktijk slaat gegevens van patiënten en medewerkers in beginsel niet op buiten de Europese Economische Ruimte (EER).

Indien de Praktijk persoonsgegevens toch buiten de EER opslaat, bijvoorbeeld omdat een Verwerker van de Praktijk daar gevestigd is, zorgt de Praktijk er voor dat de doorgifte alleen plaatsvindt als:

- de Europese Commissie heeft aangegeven dat het betreffende land een passend beschermingsniveau biedt;
- de EU standard contractual clauses zijn overeengekomen;
- het privacy shield van toepassing is; of
- een andere vrijstelling van toepassing is.

Bijlage 1

Privacy- en cookieverklaring

Uw privacy wordt door ons gerespecteerd. Adding, Praktijk voor Tandheelkunde streeft ernaar om uw privacy zo goed mogelijk te waarborgen en zal vertrouwelijk omgaan met de informatie die u bij ons aanlevert. Bij de verwerking van persoonsgegevens nemen wij de geldende wet- en regelgeving op het gebied van privacy in acht. In deze privacy- en cookieverklaring informeren wij u over de wijze waarop wij met uw gegevens omgaan.

Categorieën persoonsgegevens
Door het gebruiken van de website en de daarop beschikbare diensten laat u bepaalde gegevens bij ons achter. Dat gebeurt ook bij ons in de praktijk in het kader van de uitvoering van de behandelovereenkomst. Dat kunnen persoonsgegevens zijn. Wij bewaren en gebruiken uitsluitend de persoonsgegevens die rechtstreeks door u worden opgegeven of waarvan bij opgave duidelijk is dat ze aan ons worden verstrekt om te verwerken.

Afhankelijk van de dienst die u gebruikt kunnen wij de volgende gegevens verzamelen:

- *Naam, adres, postcode en woonplaats*
- *Geslacht;*
- *E-mailadres;*
- *Telefoonnummer, vast en/of mobiel*
- *Gegevens betreffende uw gezondheid;*
- *De naam van uw zorgverzekeraar;*
- *De naam van uw andere zorgverleners;*
- *Tijdstip van uw afspraak;*
- *Betalingsgegevens;*
- *Burgerservicenummer*

Grondslag voor gegevensverwerking
Wij mogen alleen rechtmatig persoonsgegevens van u verwerken als wij dat doen op basis van een juridische grondslag. Wij verwerken uw persoonsgegevens omdat dit noodzakelijk is voor het uitvoeren van de overeenkomst tussen u en ons, zoals neergelegd in artikel 6 lid 1 sub b van de Algemene Verordening Gegevensbescherming (AVG). Daarnaast kunnen wij uw persoonsgegevens verwerken voor een ander gerechtvaardigd belang, zoals het informeren van onze patiënten over actualiteiten of wijzigingen in onze dienstverlening. Deze grondslag is neergelegd in artikel 6 lid 1 sub f van de AVG.

Doeleinden gegevensverwerking
De persoonsgegevens die door ons worden verzameld, worden gebruikt voor de volgende doeleinden:

- Het aanmaken van een inschrijfformulier om u bij de praktijk in te schrijven;
- Het inloggen in de online praktijkagenda
- Het bijhouden van uw medisch dossier;
- Het inplannen van een afspraak;
- Het uitvoeren van een behandeling;
- Het bijhouden van door u aangegeven voorkeuren;
- Het aanmaken van een factuur die verwerkt wordt door Infomedics;
- Het verbeteren van onze dienstverlening;
- Het uitvoeren van overige, door u gevraagde, diensten.

Verstrekking van uw persoonsgegevens aan derden
Wij verstrekken uw persoonsgegevens in beginsel alleen aan derde partijen indien u daar zelf toestemming voor heeft gegeven. Gegevensverstrekking zonder uw toestemming vindt plaats indien dat noodzakelijk is om de overeenkomst tussen u en ons uit te kunnen voeren of een wettelijke verplichting ons dat voorschrijft.

Bewaartermijnen
Wij zullen uw gegevens niet langer bewaren dan noodzakelijk is voor de in deze privacy- en cookieverklaring beschreven doeleinden, tenzij dat nodig is op grond van een wettelijke verplichting. Voor het bewaren van uw medische gegevens hanteren wij de wettelijke bewaartermijn van 15 jaar uit de Wet op de geneeskundige behandelovereenkomst. Naast de WGBO houden we indien nodig ook rekening met bewaartermijnen die voortvloeien uit andere wetgeving.
Betaalgegevens worden 7 jaar bewaard.

Beveiligingsmaatregelen
Om uw gegevens zo goed mogelijk te beschermen hebben wij passende beveiligingsmaatregelen getroffen;

- De website is beveiligd via SSL, of eigenlijk TLS, herkenbaar aan https:// voor het website adres, dit is een techniek waarmee de verbinding tussen de bezoeker van een website en de server waar de website is ondergebracht wordt beveiligd middels zeer sterke encryptie. Er wordt altijd gedacht dat SSL alleen nodig is wanneer een bezoeker gegevens verstuurt via de website, maar SSL werkt twee kanten op. Met een SSL verbinding zorg je ervoor dat men niet kan meelezen met wat je naar de website verstuurt. Maar het voorkomt ook dat informatie die naar de website verstuurd wordt, of vanaf de website verzonden wordt, aangepast kan worden.
- Alle printer en usbpoorten aan de balie zijn geblokkeerd.
- Tijdens pauzes of afwezigheid is elke pc vergrendeld.
- Praktijkmedewerkers loggen in onder naam en password.
- Patiëntgegevens worden op kantoor verwerkt achter in de praktijk waar bezoekers geen toegang hebben.
- Wij gebruiken Zorgmail om uw verwijzing naar bijvoorbeeld een kaakchirurg of ziekenhuis beveiligd en versleuteld te versturen.
- Wij gebruiken in onze brieven of verwijzingen uw burgerservicenummer niet.
- Infomedics verzorgt onze facturen en werkt onder ISO9001, ISO27001 en NEN7510 certificering. Hierbij wordt voldaan aan alle eisen van privacybescherming volgens de Algemene Bevordering Gegevensbescherming.

Verwijzingen naar websites van derden (via hyperlinks)
Om u van dienst te zijn hebben wij op onze websites verwijzingen opgenomen naar websites van derden. Wij maken u er graag op attent dat wanneer u deze websites bezoekt, de voorwaarden uit de privacy verklaringen van deze derden van toepassing zijn. Wij raden u aan om de privacy verklaringen van deze websites te lezen voordat u daar verder gebruik van maakt.

Het gebruik van cookies
Voor het functioneren van onze praktijkwebsite maken wij gebruik van cookies. Cookies zijn informatiebestandjes die bij het bezoeken van een website automatisch kunnen worden opgeslagen op of uitgelezen van het device (zoals PC, tablet of smartphone) van de bezoeker. Dat gebeurt via de webbrowser op het device. Cookies zijn er in verschillende soorten. Wij maken gebruik van de volgende soorten cookies:

- analytic cookies: om te kunnen analyseren hoe onze website door bezoekers wordt gebruikt en naar aanleiding daarvan verbeteringen te kunnen doorvoeren;

Via onze website worden cookies geplaatst van het Amerikaanse bedrijf Google, als deel van de Analytics dienst. Wij gebruiken deze dienst om bij te houden en rapportages te krijgen over hoe bezoekers de website gebruiken. Wij gebruiken deze dienst niet voor ingelogde gebruikers. Wij hebben Google niet toegestaan de verkregen Analytics informatie te gebruiken voor andere Google diensten, wij laten de IP-adressen anonimiseren. De informatie die door Google wordt verzameld, wordt overgebracht naar en

opgeslagen op servers in de Verenigde Staten. Wij hebben een verwerkersovereenkomst met Google gesloten. De informatie die Google verzamelt wordt zo veel mogelijk geanonimiseerd. Wij hebben geen invloed op het gebruik van de data door Google en/of derden. Google kan deze informatie aan derden verschaffen indien zij hiertoe wettelijk worden verplicht, of voor zover derden de informatie namens Google verwerkt. Google houdt zich aan de privacybeginselen van en zijn aangesloten bij Privacy Shield van het Amerikaanse Ministerie van Economische Zaken en de Europese Commissie. Voor meer informatie over deze gegevensverwerking kunt u de privacy verklaring van Google lezen.

In uw browser kunt u de instellingen rond het gebruik van cookies desgewenst aanpassen. Ook kunt u eventueel handmatig cookies verwijderen. Dit leest u na in de handleiding van uw browser.

Uw rechten
Wanneer u persoonsgegevens aan ons heeft verstrekt, heeft u verschillende rechten die u kunt uitoefenen. Zo heeft u recht op inzage, rectificatie en het wissen van uw gegevens. Ook kunt u ons verzoeken om uw gegevens aan u of een andere partij over te dragen of om de gegevensverwerking te beperken. Het staat u daarnaast vrij om bezwaar te maken tegen een verwerking van uw gegevens. U kunt bovendien uw toestemming voor de gegevensverwerking altijd in te trekken. U kunt uw verzoek bij ons kenbaar maken door ons een e-mail te sturen aan info@adding.nl of door telefonisch contact met ons op te nemen via: 0516-513739. Wij streven ernaar om binnen 1 maand op uw verzoek te reageren.

Klacht indienen bij de Autoriteit persoonsgegevens
Mocht u onverhoopt niet tevreden zijn over de wijze waarop wij met uw gegevens omgaan, dan kunt u een klacht hierover indienen bij de Autoriteit persoonsgegevens. De contactgegevens van de Autoriteit persoonsgegevens vindt u hier:
https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/klacht-over-gebruik-persoonsgegevens

Wijzigingen in deze privacy- en cookieverklaring
Wij behouden ons het recht voor om deze privacy- en cookieverklaring aan te passen. Deze wijzigingen zullen via onze praktijkwebsite bekend worden gemaakt. Wij raden u daarom aan om deze verklaring regelmatig te raadplegen, zodat u van eventuele wijzigingen op de hoogte bent.

Onze contactgegevens
Heeft u nog vragen of opmerkingen na het lezen van deze privacy- en cookieverklaring? Dan kunt u hiervoor contact met ons opnemen via de onderstaande contactgegevens:

Géke Lassche of Nynke Adding, praktijkmanagers van Adding, Praktijk voor Tandheelkunde, 0516-513739.

****

Bijlage 2

Privacy- en cookieverklaring

Uw privacy wordt door ons gerespecteerd. Adding, Praktijk voor Tandheelkunde streeft ernaar om uw privacy zo goed mogelijk te waarborgen en zal vertrouwelijk omgaan met de informatie die u bij ons aanlevert. Bij de verwerking van persoonsgegevens nemen wij de geldende wet- en regelgeving op het gebied van privacy in acht. In deze privacy- en cookieverklaring informeren wij u over de wijze waarop wij met uw gegevens omgaan.

Categorieën persoonsgegevens

Door het gebruiken van de website en de daarop beschikbare diensten laat u bepaalde gegevens bij ons achter. Dat gebeurt ook bij ons in de praktijk in het kader van de uitvoering van de behandelovereenkomst. Dat kunnen persoonsgegevens zijn. Wij bewaren en gebruiken uitsluitend de persoonsgegevens die rechtstreeks door u worden opgegeven of waarvan bij opgave duidelijk is dat ze aan ons worden verstrekt om te verwerken.

Verwerkersovereenkomst

De ondergetekenden:

Adding, Praktijk voor Tandheelkunde gevestigd aan Snellingerdijk 39a, 8431 EJ te Oosterwolde ingeschreven in het register van de Kamer van Koophandel onder nummer 01078498 hierna te noemen: “Opdrachtgever” / Verwerkingsverantwoordelijke (in de zin van de AVG)

en

[Naam Verwerker], gevestigd aan [adres],[postcode] te [woonplaats] en ingeschreven in het register van de Kamer van Koophandel onder nummer [KVK nummer], hierna te noemen “Opdrachtnemer” / Verwerker (in de zin van de AVG)

hierna gezamenlijk ook aan te duiden als: “Partijen” en afzonderlijk als “Partij”.

Overwegende dat

(a) Opdrachtnemer diensten verricht ten behoeve van Opdrachtgever, zoals beschreven in de Hoofdovereenkomst [naam en datum Hoofdovereenkomst] met nummer [contract/referentie nummer] ;
(b) Opdrachtnemer zal bij het uitvoeren van de Hoofdovereenkomst gegevens verwerken waarvoor Opdrachtgever verantwoordelijk blijft. Opdrachtnemer verwerkt gegevens louter in opdracht van Opdrachtgever en niet voor eigen doeleinden. Op deze gegevensverwerking zijn de bepalingen van toepassing uit de Algemene Verordening Gegevensbescherming (EU 2016/679), hierna de “AVG”.

(c) Partijen wensen middels deze overeenkomst, hierna te noemen: de "Verwerkersovereenkomst", afspraken met betrekking tot de verwerking van persoonsgegevens in het kader van de te verlenen diensten vast te leggen conform artikel 28 lid 3 AVG;
(d) Voor zover van toepassing, vervangt deze Verwerkersovereenkomst de eerdere overeenkomst(-en) van gelijke strekking die tussen Partijen zijn gesloten.

VERKLAREN TE ZIJN OVEREENGEKOMEN ALS VOLGT:

Artikel 1. Definities

1.1 Voor zover begrippen met een hoofdletter niet afzonderlijk gedefinieerd zijn in deze Verwerkersovereenkomst, gelden de definities zoals genoemd in de Hoofdovereenkomst, welke overeenkomst onder overweging (a) nader is benoemd. Begrippen uit de Algemene Verordening Gegevensbescherming (AVG), zoals "verwerken", "persoonsgegevens", "verwerkingsverantwoordelijke" en "verwerker" hebben de betekenis die daaraan is gegeven in de AVG.

Artikel 2. Onderwerp van deze Verwerkersovereenkomst

2.1 Opdrachtnemer kan gedurende de uitvoering van de in artikel 1 van deze Verwerkersovereenkomst genoemde Hoofdovereenkomst ten behoeve van Opdrachtgever en ter voldoening aan enige wettelijke verplichting persoonsgegevens verwerken. Een overzicht van de categorieën Persoonsgegevens en de doeleinden waarvoor de persoonsgegevens ten behoeve van Opdrachtgever worden verwerkt is opgenomen in Annex 1 bij deze Verwerkersovereenkomst.

Artikel 3. Uitvoering verwerking

3.1 Opdrachtnemer zal optreden als Verwerker en Opdrachtgever als Verwerkingsverantwoordelijke in de zin van de AVG.
3.2 Opdrachtnemer garandeert dat hij ten behoeve van Opdrachtgever uitsluitend persoonsgegevens zal verwerken voor zover dit noodzakelijk is voor de uitvoering van de onder de in artikel 1 van deze Verwerkersovereenkomst genoemde Hoofdovereenkomst. Overige verwerkingen zullen uitsluitend worden uitgevoerd in expliciete opdracht van Opdrachtgever of als daartoe een wettelijke verplichting bestaat na informeren van en onder verantwoordelijkheid van Opdrachtgever. In geen geval zal Opdrachtnemer persoonsgegevens verwerken voor eigen doeleinden.
3.3 Opdrachtnemer zal alle redelijke verzoeken en/of instructies van Opdrachtgever in verband met de verwerking van de persoonsgegevens opvolgen. Opdrachtnemer stelt Opdrachtgever onmiddellijk op de hoogte indien naar zijn oordeel verzoeken of instructies in strijd zijn met de toepasselijke wetgeving met betrekking tot de verwerking van persoonsgegevens.
3.4 Opdrachtnemer zal de persoonsgegevens aantoonbaar, op behoorlijke en zorgvuldige wijze en in overeenstemming met de op hem als Verwerker op grond van de AVG en overige wetgeving rustende verplichtingen verwerken. Indien er sprake is van het verwerken van bijzondere persoonsgegevens volgens artikel 9 AVG zal Opdrachtnemer zich tevens houden aan de bepalingen van boek 7, titel 7, afdeling 5 BW (de Wet geneeskundige behandelingsovereenkomst, Wgbo) indien deze van toepassing zijn op Opdrachtgever. Partijen sluiten de Hoofdovereenkomst om de expertise die Opdrachtnemer heeft als het gaat om het beveiligen en het verwerken van Persoonsgegevens te gebruiken voor de doeleinden die uiteengezet zijn in Annex 1 bij deze Verwerkersovereenkomst. Opdrachtnemer is gehouden om, met inachtneming van hetgeen in deze Verwerkersovereenkomst is

bepaald, naar eigen inzicht de middelen aan te wenden die hij noodzakelijk acht om die doeleinden na te streven.

3.5 Opdrachtnemer zal, tenzij hij hiervoor uitdrukkelijke voorafgaande schriftelijke toestemming heeft verkregen van Opdrachtgever, geen persoonsgegevens verwerken of laten verwerken door hemzelf of door derden in landen buiten de Europese Economische Ruimte ("EER") zonder een passend beschermingsniveau. Opdrachtnemer stelt de in Annex 4 genoemde medewerker van Opdrachtgever onmiddellijk schriftelijk op de hoogte van alle (geplande) permanente of tijdelijke doorgiftes van persoonsgegevens naar een land buiten de Europese Economische Ruimte en zal pas uitvoering geven aan dergelijke (geplande) doorgiftes na schriftelijke toestemming van Opdrachtgever. Opdrachtgever heeft te allen tijde het recht om aanvullende voorwaarden te verbinden aan haar toestemming voor een dergelijke verwerking.

3.6 Onverminderd enige andere contractuele geheimhoudingsverplichting die op Opdrachtnemer rust, garandeert Opdrachtnemer dat hij alle persoonsgegevens als strikt vertrouwelijk zal behandelen en dat hij al zijn werknemers, vertegenwoordigers en/of onderaannemers ('sub-verwerkers') die betrokken zijn bij de verwerking van persoonsgegevens ook van deze geheimhoudingsverplichting op de hoogte zal stellen.

3.7 Opdrachtnemer zal, binnen zijn invloedsfeer, zijn volledige en tijdige medewerking verlenen aan Opdrachtgever om:

(i) na goedkeuring van en in opdracht van Opdrachtgever betrokkenen toegang te laten krijgen tot de hun betreffende persoonsgegevens;
(ii) persoonsgegevens te verwijderen of te corrigeren;

(iii) aan te tonen dat persoonsgegevens verwijderd of gecorrigeerd zijn indien zij incorrect zijn (of, ingeval Opdrachtgever het er niet mee eens is dat persoonsgegevens incorrect zijn, het feit vast te leggen dat de betrokkene zijn persoonsgegevens als incorrect beschouwt);
(iv) de betreffende persoonsgegevens aan Opdrachtgever dan wel aan een door de Opdrachtgever aangewezen derde te verstrekken in een gestructureerde, gangbare en machine leesbare vorm en;
(v) Opdrachtgever anderszins in de gelegenheid te stellen om aan zijn verplichtingen onder de AVG of andere toepasselijke wetgeving op het gebied van verwerking van persoonsgegevens te voldoen.

3.8 Opdrachtnemer zal de persoonsgegevens betreffende Opdrachtgever strikt gescheiden opslaan en verwerken van de persoonsgegevens die hij voor zichzelf of namens derde partijen verwerkt.

Artikel 4. Beveiliging persoonsgegevens & controle

4.1 Opdrachtnemer zal passende technische en organisatorische beveiligingsmaatregelen nemen, die op grond van de AVG, waaronder in ieder geval artikel 32 AVG, vereist zijn.

4.2 Opdrachtnemer heeft te allen tijde een passend, geschreven beveiligingsbeleid conform ISO27001 en/of NEN7510 geïmplementeerd voor de verwerking van persoonsgegevens. Een beschrijving van de beveiligingsmaatregelen en gehanteerde normen is opgenomen in Annex 2 bij deze Verwerkersovereenkomst.

4.3 Opdrachtgever heeft het recht toe te laten zien op de naleving van de hiervoor onder 4.1 en 4.2 genoemde maatregelen door een onafhankelijke, deskundige derde partij. Opdrachtnemer stelt Opdrachtgever, indien Opdrachtgever daarom verzoekt, hiertoe in elk geval eenmaal per jaar in de gelegenheid op een door Partijen in gezamenlijk overleg nader te bepalen tijdstip en verder indien Opdrachtgever daar aanleiding toe ziet naar aanleiding van (vermoeden van) informatie- of privacy-incidenten, zulks te laten controleren door een onafhankelijke, deskundige derde partij. Opdrachtnemer zal eventuele door Opdrachtgever naar aanleiding van een dergelijke controle in redelijkheid gegeven instructies tot aanpassing van het beveiligingsbeleid binnen een redelijke termijn opvolgen.

4.4 Opdrachtnemer zal in alle redelijkheid aan het onder 4.3 hiervoor bedoelde onderzoek haar medewerking verlenen.

4.5 Kosten voortvloeiende uit een onderzoek als bedoeld onder 4.3 zijn voor rekening van Opdrachtgever, daaronder uitdrukkelijk *niet* inbegrepen is een vergoeding voor de tijd die Opdrachtnemer moet inzetten voor het uitvoeren van dit onderzoek. Voor zover uit het onderzoek naar voren komt dat Opdrachtnemer aanpassingen zal moeten doen die noodzakelijk zijn voor de naleving van de verplichtingen uit deze Verwerkersovereenkomst, komen de daarmee gepaard gaande kosten voor rekening van Opdrachtnemer.

4.6 Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Opdrachtnemer zal daarom de maatregelen zoals geïmplementeerd op basis van dit artikel 4 voortdurend evalueren en verscherpen, aanvullen of verbeteren om te blijven voldoen aan zijn verplichtingen onder dit artikel.

Artikel 5. Monitoring beveiliging en afspraken bij datalekken

5.1 Opdrachtnemer zal actief monitoren op inbreuken op de beveiligingsmaatregelen en over de resultaten van de monitoring, voor zover relevant voor Verwerkingsverantwoordelijke, in overeenstemming met dit artikel 5 rapporteren aan Opdrachtgever, voor zover relevant voor Opdrachtgever.

5.2 Zodra zich een incident met betrekking tot de verwerking van de persoonsgegevens voordoet, heeft voorgedaan of zou kunnen voordoen, is Opdrachtnemer verplicht Opdrachtgever daarvan onverwijld, doch binnen 24 uur na ontdekking, in kennis te stellen en daarbij alle relevante informatie te verstrekken om aan de verplichtingen uit artikel 33 AVG te kunnen voldoen, waaronder in ieder geval:

a. de aard van het incident;
b. het risico dat gegevens onrechtmatig verwerkt zijn of kunnen worden;
c. de (mogelijk) getroffen gegevens en tot welke categorie die gegevens behoren;
d. de (mogelijk) getroffen betrokkenen;
e. de geconstateerde en vermoedelijke gevolgen van het incident;
f. de maatregelen die getroffen zijn of zullen worden om het incident op te lossen dan wel de gevolgen/schade zoveel mogelijk te beperken;

5.3 Opdrachtnemer is, onverminderd de overige verplichtingen uit dit artikel, verplicht om de eventuele negatieve gevolgen die voortvloeien uit een incident zo snel mogelijk ongedaan te

maken dan wel de verdere gevolgen te minimaliseren. Opdrachtnemer en Opdrachtgever treden hierover met elkaar in overleg om nadere afspraken te maken.

5.4 Opdrachtnemer zal Opdrachtgever te allen tijde haar medewerking verlenen en zal de instructies van Opdrachtgever opvolgen, met als doel Opdrachtgever in staat te stellen een deugdelijk onderzoek te verrichten naar het incident, een correcte respons te formuleren en passende vervolgstappen te nemen ten aanzien van het incident, waaronder begrepen het informeren van de Autoriteit persoonsgegevens (AP) en/of de betrokkene zoals bepaald in artikel 5.8.

5.5 Onder “incident” wordt in elk geval het volgende verstaan:

(a) een klacht of (informatie)verzoek van een natuurlijk persoon via Opdrachtgever, met betrekking tot de verwerking van persoonsgegevens door Opdrachtnemer;

(b) een onderzoek naar of beslaglegging door overheidsfunctionarissen op de persoonsgegevens of een vermoeden dat dit gaat plaatsvinden;

(c) iedere ongeautoriseerde toegang, verwerking, verwijdering, verminking, verlies of enige vorm van onrechtmatige verwerking van de persoonsgegevens;

(d) een inbreuk op de beveiliging en/of de vertrouwelijkheid, zoals uiteengezet in artikel 3 en 4 van deze Verwerkersovereenkomst, althans ieder ander incident, die/dat leidt (of mogelijk leidt) tot onopzettelijke of

onrechtmatige vernietiging, verlies, wijziging, onbevoegde openbaarmaking van – of toegang tot – de persoonsgegevens, of enige aanwijzing dat een dergelijke inbreuk zal plaatsvinden of heeft plaatsgevonden.

5.6 Opdrachtnemer zal te allen tijde geschreven procedures voorhanden hebben die hem in staat stellen om Opdrachtgever van een onmiddellijke reactie over een incident te voorzien, en om effectief samen te werken met Opdrachtgever om het incident af te handelen en zal Opdrachtgever voorzien van een exemplaar van dergelijke procedures indien Opdrachtgever daarom verzoekt.

5.7 Meldingen die worden gedaan op grond van dit artikel worden onverwijld gericht aan de in Annex 4 opgenomen werknemer van Opdrachtgever of, indien relevant, aan een andere door Opdrachtgever tijdens de duur van deze Verwerkersovereenkomst schriftelijk bekend gemaakte andere werknemer van Opdrachtgever.

5.8 Opdrachtgever zal, indien naar haar oordeel noodzakelijk en zover relevant voor het betreffende incident, betrokkenen en de AP informeren over incidenten. Het is Opdrachtnemer niet toegestaan informatie te verstrekken over incidenten aan betrokkenen of andere derde partijen, behoudens voor zover Opdrachtnemer daartoe wettelijk verplicht is.

5.9 Uitsluitend indien de Opdrachtgever daarvoor uitdrukkelijke toestemming geeft, zal Opdrachtnemer de eerste melding van een incident aan de AP doen. Over deze melding en over de voortgang daarvan, houdt de Opdrachtnemer de Opdrachtgever voortdurend op te hoogte.

Artikel 6. Inschakeling onderaannemers ('sub-verwerkers')

6.1 Opdrachtnemer zal zijn activiteiten die (deels) bestaan uit het verwerken van persoonsgegevens of vereisen dat persoonsgegevens verwerkt worden niet uitbesteden aan een derde partij ('sub-verwerker') zonder voorafgaande schriftelijke toestemming van Opdrachtgever.

6.2 Opdrachtnemer zal aan de door hem ingeschakelde derde dezelfde of strengere verplichtingen opleggen als voor hemzelf uit deze Verwerkersovereenkomst en de wet voortvloeien en ziet toe op de naleving daarvan door de derde. De betreffende afspraken met de derde zullen schriftelijk worden vastgelegd. Opdrachtnemer zal Opdrachtgever op verzoek afschrift verstrekken van deze overeenkomst(en) voor zover relevant voor naleving van deze Verwerkersovereenkomst.

6.3 Niettegenstaande de toestemming van Opdrachtgever voor het inschakelen van een derde partij blijft Opdrachtnemer volledig aansprakelijk jegens Opdrachtgever voor de gevolgen van het uitbesteden van werkzaamheden aan een derde. De toestemming van Opdrachtgever voor het uitbesteden van werkzaamheden aan een derde partij laat onverlet dat voor de inzet van sub-verwerkers in een land buiten de Europese Economische Ruimte zonder een passend beschermingsniveau toestemming vereist is in overeenstemming met artikel 3.5 van deze Verwerkersovereenkomst.

6.4 Opdrachtgever geeft hierbij toestemming voor het inschakelen van de in Annex 3 opgenomen sub-verwerker(s) door Opdrachtnemer. Partijen zorgen ervoor dat deze bijlage up to date blijft. Opdrachtnemer zal Opdrachtgever direct informeren wanneer een overeenkomst met een sub-verwerker is beëindigd.

Artikel 7. Aansprakelijkheid

7.1 Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen. De in dit artikel 7 geregelde aansprakelijkheid heeft uitsluitend betrekking op boetes en schade ten gevolge van een verwijtbare tekortkoming in de naleving van het bepaalde in deze Verwerkersovereenkomst. Voor dergelijke tekortkomingen geldt geen beperking van aansprakelijkheid, tenzij anders schriftelijk overeengekomen.

7.2 Opdrachtnemer vrijwaart Opdrachtgever tegen claims en aanspraken van derden voor schade (beweerdelijk) veroorzaakt door wederrechtelijke verwerking van persoonsgegevens of door enige daad die in strijd is met de AVG, andere toepasselijke wettelijke bepalingen of met deze Verwerkersovereenkomst of de Hoofdovereenkomst, alsmede voor boetes opgelegd door bevoegde autoriteiten als gevolg van voornoemde daad. Het voorgaande geldt niet indien dergelijke claims het gevolg zijn van een toerekenbare tekortkoming van Opdrachtgever.

7.7 Partijen zorgen ervoor dat zij zich adequaat verzekerd hebben en houden, zodat er sprake is van een afdoende dekking van de aansprakelijkheid als genoemd in dit artikel.

Artikel 8. Duur, beëindiging en wijziging

8.1 Deze Verwerkersovereenkomst gaat in op [datum] en de duur van deze Verwerkersovereenkomst is gelijk aan de duur van de in artikel 1 genoemde Hoofdovereenkomst.

8.2 Na ondertekening door beide Partijen zal deze Verwerkersovereenkomst onderdeel uitmaken van de Hoofdovereenkomst en zijn deze beide overeenkomsten onlosmakelijk met elkaar verbonden. Dat wil zeggen dat beëindiging van de Verwerkersovereenkomst, op welke grond dan ook (opzegging/ontbinding), tot gevolg heeft dat de Hoofdovereenkomst eveneens op dezelfde grond beëindigd wordt (en vice versa), tenzij partijen in voorkomend geval anders overeenkomen.

8.3 Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst gelden. Tot deze bepalingen behoren onder meer die welke voortvloeien uit de bepalingen betreffende geheimhouding, aansprakelijkheid en toepasselijk recht.

8.4 Ieder der partijen is gerechtigd, onverminderd hetgeen daartoe bepaald is in de Hoofdovereenkomst, de uitvoering van deze Verwerkersovereenkomst en de daarmee samenhangende Hoofdovereenkomst op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang te ontbinden, indien:

(a) de andere partij wordt ontbonden of anderszins ophoudt te bestaan;

(b) de andere partij aantoonbaar tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die ernstige toerekenbare tekortkoming niet binnen redelijke en in samenspraak vastgestelde termijn is hersteld na een daartoe strekkende schriftelijke ingebrekestelling;

(c) een partij in staat van faillissement wordt verklaard of surséance van betaling aanvraagt.

8.5 Opdrachtnemer informeert Opdrachtgever onverwijld indien de situatie dreigt te ontstaan zoals benoemd in het vorige lid van dit artikel onder (c), zodat Opdrachtgever tijdig een besluit kan nemen over het terugvorderen van persoonsgegevens.

8.6 Opdrachtgever is gerechtigd deze Verwerkersovereenkomst en de Hoofdovereenkomst per direct te ontbinden indien Opdrachtnemer te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of de rechtspraak aan de verwerking van de persoonsgegevens worden gesteld. Artikel 9.2 is van overeenkomstige toepassing.

8.7 Wijzigingen van deze Verwerkersovereenkomst zijn uitsluitend geldig indien deze tussen Partijen schriftelijk zijn overeengekomen.

8.8 Partijen zullen deze Verwerkersovereenkomst in ieder geval wijzigen indien daarvoor een aanleiding bestaat op basis van ontwikkelingen in de jurisprudentie en/of relevante wet- en regelgeving.

Artikel 9. Bewaartermijnen, teruggave en vernietiging van Persoonsgegevens

9.1 Opdrachtnemer bewaart de persoonsgegevens niet langer dan strikt noodzakelijk voor de doelen als omschreven in Annex 1 en in geen geval langer dan tot het einde van deze Verwerkersovereenkomst

of, indien tussen partijen een bewaartermijn is overeengekomen, niet langer dan deze termijn.

9.2 Bij beëindiging van de Verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van Opdrachtgever zal

Opdrachtnemer, naar keuze van Opdrachtgever, kosteloos de persoonsgegevens onherroepelijk vernietigen of teruggeven aan Opdrachtgever. Op verzoek van Opdrachtgever verstrekt Opdrachtnemer bewijs van het feit dat de gegevens vernietigd of verwijderd zijn. Indien teruggave, vernietiging of verwijdering niet mogelijk zijn, stelt Opdrachtnemer Opdrachtgever daarvan onmiddellijk op de hoogte. In dat geval garandeert Opdrachtnemer dat hij de persoonsgegevens vertrouwelijk zal behandelen en niet langer zal verwerken.

9.3 Bij het einde van de Verwerkersovereenkomst zal Opdrachtnemer alle, bij haar bekende en door haar ingeschakelde derden die betrokken zijn bij het verwerken van persoonsgegevens op de hoogte stellen van de beëindiging van de Verwerkersovereenkomst. De verplichtingen uit artikel 9.2 zijn van overeenkomstige toepassing op de deze derden. Opdrachtnemer zal waarborgen dat alle betrokken derden hieraan uitvoering zullen geven.

Artikel 10. Slotbepalingen

10.1 De overwegingen en bijlagen maken onderdeel uit van deze Verwerkersovereenkomst.

10.2 In het geval van strijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en bepalingen uit de in artikel 1 genoemde Hoofdovereenkomst zullen de bepalingen van de Verwerkersovereenkomst leidend zijn.

10.3 In geval van nietigheid c.q. vernietigbaarheid van één of meer bepalingen uit deze Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.

10.4 Op deze Verwerkersovereenkomst is louter Nederlands recht van toepassing.

10.5 Eventuele conflicten zullen eerst met elkaar besproken worden waarbij beide partijen zich inspannen om deze in goed overleg met elkaar op te lossen.

10.6 Geschillen over of in verband met deze Verwerkersovereenkomst worden uitsluitend voorgelegd aan de bevoegde rechter in het arrondissement van de Opdrachtgever.

10.7 In alle gevallen waarin deze Verwerkersovereenkomst niet voorziet beslissen Partijen in onderling overleg.

Adding, Praktijk voor Tandheelkunde
_____

Naam: ……..
……..
Functie: ……
……
Plaats: ……
……..
Datum: ……
……

En

[Opdrachtnemer]

_____

Naam: ……..
……..

Functie: ……
……
Plaats: ……
……..
Datum: ……
……

Aantal bijlagen bij deze Verwerkersovereenkomst (4):

Annex 1 – Te verwerken persoonsgegevens en doeleinden
Annex 2 – Beveiligingsmaatregelen
Annex 3 – Sub-verwerker(s)
Annex 4 – Contactgegeven

ANNEX 1: Te verwerken persoonsgegevens en doeleinden

Deze bijlage maakt onderdeel uit van de Verwerkersovereenkomst en dient dan ook aan de Verwerkersovereenkomst te worden gehecht en tevens door Partijen te worden geparafeerd.

Hier dient te worden uitgewerkt:

- Welke persoonsgegevens Opdrachtnemer in opdracht van Opdrachtgever gaat verwerken ter uitvoering van de diensten zoals overeengekomen in de Hoofdovereenkomst tussen Partijen (bijvoorbeeld NAW, telefoonnummer, beroep, financiële data, geboortedatum etc.);

- De doeleinden waarvoor Opdrachtnemer persoonsgegevens zal gaan verwerken zoals eveneens van belang voor de uitvoering van de diensten zoals overeengekomen in de Hoofdovereenkomst tussen Partijen (dus hier zo concreet mogelijk beschrijven wat er met de gegevens wordt gedaan en met welk doel);

- De wijze waarop Opdrachtnemer de persoonsgegevens zal gaan verwerken (welke middelen en/of systemen worden hiervoor gebruikt);

- De bewaartermijnen die zullen worden gehanteerd voor de betreffende persoonsgegevens.

Toelichting:

<u>Persoonsgegevens</u>

De definitie van persoonsgegevens is onder de AVG erg ruim. Hier valt '*alle informatie onder over een geïdentificeerde of identificeerbare natuurlijke persoon'*. Uit de informatie kan direct of indirect worden afgeleid op wie het betrekking heeft.

De AVG maakt onderscheid tussen verschillende categorieën van persoonsgegevens. Medische gegevens, zoals tandheelkundige informatie over patiënten, en bijvoorbeeld het BSN worden als gevoelig beschouwd en kwalificeren daarmee onder de AVG als '*bijzondere persoonsgegevens'*. Voor dit type persoonsgegevens dient goed te worden gekeken naar de beveiligingsmaatregelen om deze gegevens te beschermen. Deze gegevens dienen streng te worden beveiligd.

<u>Doeleinden</u>

Onder de AVG gelden de beginselen van '*doelbinding*' en '*gegevensminimalisatie*'. Dit brengt mee dat persoonsgegevens alleen

mogen worden verwerkt voor concrete, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en dat daarnaast niet meer gegevens mogen worden verwerkt dan noodzakelijk is voor die vastgestelde doeleinden.

Inzicht in systemen/middelen in verband met beveiligingsmaatregelen

Op de Opdrachtgever/Verwerkingsverantwoordelijke rust de verplichting om passende technische en organisatorische maatregelen te treffen om de persoonsgegevens te beveiligen en te verwerken in overeenstemming met de AVG. Opdrachtgever/Verwerkingsverantwoordelijke kan alleen met Verwerkers afspraken maken die voldoende garanties kunnen bieden met betrekking tot het toepassen van technische en organisatorische maatregelen. Daarom is het van belang dat door de Opdrachtnemer/Verwerkingsverantwoordelijke inzichtelijk wordt gemaakt met welke systemen wordt gewerkt of welke middelen worden ingezet en welke beveiligingsmaatregelen worden genomen (zie hierna in Annex 2).

Bewaartermijnen

Het is raadzaam om in onderling overleg te bepalen welke bewaartermijnen voor welke persoonsgegevens zullen worden gehanteerd. De AVG noemt geen concrete bewaartermijn, maar kent wel een '*opslagbeperking*'. Dit houdt in dat persoonsgegevens niet langer bewaard mogen worden dan nodig is voor het doeleinde waarvoor zij zijn verwerkt.

ANNEX 2: Beveiligingsmaatregelen

Deze bijlage maakt onderdeel uit van de Verwerkersovereenkomst en dient dan ook aan de Verwerkersovereenkomst te worden gehecht en tevens door Partijen te worden geparafeerd.

Hier dient te worden uitgewerkt welke beveiligingsmaatregelen Opdrachtnemer/Verwerker heeft getroffen om een veilige gegevensverwerking te kunnen waarborgen.

Ook kan hier worden vermeld, voor zover dat het geval is, aan welke normen voor informatiebeveiliging door Opdrachtnemer/Verwerker wordt voldaan (bijvoorbeeld de NEN7510).

Toelichting:

Het verdient aanbeveling om de beveiligingsmaatregelen hier zo concreet mogelijk te benoemen. Voorbeelden van beveiligingsmaatregelen zijn:

- tijdige installatie van beveiligingsupdates en patches ter zake van de gebruikte software;
- logische toegangscontrole, gebruik makend van wachtwoorden;
- fysieke maatregelen voor toegangsbeveiliging;
- het bewaren van de (algemene) Windows logging;
- het opstellen van een protocol waarin de handelingen die met betrekking tot persoonsgegevens worden uitgevoerd worden beschreven en de waarborgen die daarbij in acht worden genomen;
- encryptie (versleuteling) van digitale bestanden met Persoonsgegevens bij opslag (beheer) en het verzenden van deze bestanden (werkbestanden daarvan uitgezonderd);
- organisatorische maatregelen voor toegangsbeveiliging;
- beveiliging van netwerkverbindingen via Secure Socket Layer (SSL) technologie;
- doelgebonden toegangsbeperkingen;
- controle op toegekende bevoegdheden.

Sommige Verwerkers hebben de door hen getroffen beveiligingsmaatregelen al in een apart document schriftelijk vastgelegd. Dit document kan dan eventueel ook als Annex 2 bij deze Verwerkersovereenkomst worden gevoegd (mits daarin de beveiligingsmaatregelen concreet en duidelijk staan beschreven en up to date zijn).

ANNEX 3: Sub – verwerker(s)

Deze bijlage maakt onderdeel uit van de Verwerkersovereenkomst en dient dan ook aan de Verwerkersovereenkomst te worden gehecht en tevens door Partijen te worden geparafeerd.

Hier kan een lijst worden opgenomen van de door de Opdrachtnemer ingeschakelde derden, de 'sub-verwerkers'. De adres/contactgegevens van deze sub-verwerkers kan hier worden vermeld, maar bijvoorbeeld ook of er met deze sub-verwerkers een verwerkersovereenkomst is gesloten en aan welke beveiligingsnormen deze sub-verwerkers zich houden.

Toelichting:

Onder de AVG (artikel 28 lid 4) is bepaald dat Sub-verwerkers die worden ingeschakeld door de Verwerker aan dezelfde verplichtingen op het gebied van gegevensbescherming gehouden zijn als is overeengekomen tussen de Verwerker en de Verwerkingsverantwoordelijke. Daarom is het van belang dat ook tussen Verwerker en Sub-verwerker goede afspraken worden gemaakt.

ANNEX 4: Contactgegevens

Deze bijlage maakt onderdeel uit van de Verwerkersovereenkomst en dient dan ook aan de Verwerkersovereenkomst te worden gehecht en tevens door Partijen te worden geparafeerd.

Hier kunnen de contactgegevens worden vermeld van beide partijen in geval er sprake is van een beveiligingsincident of een datalek. Dit kan eventueel de Functionaris Gegevensbescherming (FG) zijn, voor zover die binnen de organisatie is aangesteld.

Neem hier in ieder geval op de naam, functie, e-mailadres en telefoonnummer(s) van de betreffende contactpersonen.

Toelichting:

Om snel te kunnen handelen en passende maatregelen te kunnen nemen in geval van een beveiligingsincident of datalek, is het raadzaam om binnen de organisatie van zowel de Opdrachtgever als Opdrachtnemer een vaste medewerker aan te wijzen met wie er in een dergelijke situatie contact kan worden opgenomen. Deze medewerker kan dan ook de afgesproken termijnen bewaken.

Het is tevens aan te raden om een extra persoon als ‘achterwacht’ aan te wijzen en ook van die persoon hier de contactgegevens op te nemen. Bij ziekte of afwezigheid van de primaire contactpersoon is er dan een tweede persoon als aanspreekpunt beschikbaar.

Bij uitdiensttreding van bovengenoemde medewerker dient uiteraard deze contactenmatrix in onderling overleg te worden ge-update.

Bijlage 3

<Pa.Titulatuur> <Pa.Naam patient>
<Pa.Adres>
<Pa.Postcd> <Pa.Woonplaats>

Adding, praktijk voor Tandheelkunde
Snellingerdijk 39a
8431 EJ Oosterwolde
0516-513739

<Me.Woonplaats>, <Al.Datum>

Onderwerp: data lek

<Pa.Aanhef>,

Onlangs is er in onze praktijk sprake geweest van een zogenoemd datalek
van gegevens waar mogelijk uw persoonsgegevens bij betrokken zijn.

Inmiddels is dit incident gemeld aan de Autoriteit Persoonsgegevens.
We hebben de volgende maatregelen genomen:

-

In de toekomst zullen we de volgende maatregelen nemen om herhaling van te voorkomen;

-

We bieden onze oprecht gemeende excuses aan voor dit data lek.

Met vriendelijke groet,