INTERN PRIVACYBELEID

VOOR DE VERWERKING VAN PERSOONSGEGEVENS

AVT Kliniek b.v

1. INTRODUCTIE

Dit is het privacybeleid (hierna: het "Privacybeleid") van AVT Kliniek b.v (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 halfjaarlijks 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 hebben de tandartsassistente, mondhygiëniste, de tandarts en de administratiemedewerker toegang tot het register. Dit is noodzakelijk voor het verwerken van uw gegevens en bijhouden van patiëntendossier.

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 [Exquise] (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 daar van tevoren van op de hoogte gebracht.

Veilig Incident Melden (VIM)

Binnen de praktijk is W. Malikzad tandarts/eigenaar 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 of digitaal 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 personeelsdossier digitaal in cloud (google drive) en locaal netwerk . Deze gegevens worden in eerste instantie gebruikt voor het vaststellen en uitbetalen van het salaris van de medewerkers. Hiervoor maakt de Praktijk gebruik van het salarisadministratiekantoor Hilversum accountant kantoor

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 Praktijkmanager en praktijk eigenaar 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 local netwerk en cloud (google drive).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 verwezen naar privacy statement en wordt er voor akkoord getekend. Het privacy statement is als bijlage verstuurd via de mail na de inschrijving. Op verzoek dan de privacy verklaring uitgeprint worden en meegegeven worden aan de patiënt tijdens het invullen van gezondheidsformulier.

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. Het gebruik van persoonsgegevens is vastgelegd in het werknemers privacybeleid van de Praktijk dat als Bijlage X aan dit Privacybeleid is gehecht

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 W. Malikzad via wm@avtkliniek.nl Verzoeken en alle overige afhandeling worden opgeslagen in patiëntendossier van desbetreffende patiënt of in apart mailbox map van de ontvanger.

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.

W. Malikzad/ tandarts eigenaar 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. Dit verslag kan worden 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 aan dit privacybeleid gehecht.

In de Praktijk wordt van de volgende Verwerkers gebruikgemaakt: hieronder zijn voorbeelden opgenomen, deze kunnen worden aangepast of aangevuld aan de omstandigheden van de Praktijk

- [Vertimart] in het kader van onderhoud en support
- [SiteGround web hosting] in het kader van hosting
- [Refa ICT] in het kader van automatisering en onderhoud en support daarop
- VECOZO voor controle van patiëntgegevens bij de zorgverzekeraar en/of het verzenden van gegevens aan zorgverzekeraar
- Incassobureaus De Nederlanden factoringmaatschappij, Intelly voor de facturatie en inning van facturen
- Outlook of Zorgmail in het kader van de verzending van gegevens
- Hilversum accountant in het kader van het vaststellen en uitbetalen van het salaris
- Intero in het kader van onderhoud en support (op afstand)
- Excent tandtechniek, Subliem tandtechiek, Balans tnadtechniek in het kader van het produceren van onder meer kronen
- Sirona voor het maken rontgen foto's OPT en RSP , VisieQuick van Lamoral] in het kader van hosting en/of onderhoud en support
- Henrij Schein, Dental Bauer, Beste Dental buy, VGT, Dental Rules voor onderhoud/support.

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.
- Persoonsgegevens worden niet op USB sticks of andere mobiele dragers gekopieerd tenzij de persoonsgegevens versleuteld worden
- Alleen assistentes, baliemedewerkster en de tandartsen hebben toegang tot de patiëntgegevens
- Alleen de praktijkeigenaar en praktijk manager heeft 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 Praktijk
- 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 passen/druppels

[optioneel: teneinde de veiligheid van patiënten en medewerkers te garanderen zijn er (zichtbaar en/of onzichtbaar) camera's geplaatst in en buiten de Praktijk. Aan de hand van deze camera's 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. Deze camerabeelden kunnen vervolgens door de Praktijk als bewijsmateriaal worden aangewend.]

Binnen de Praktijk worden elke dagelijks 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 W. Malikzad via wm@avtkliniek.nl . W. Malikzad 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 X 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 de praktijk netwerk.

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.