

Privacybeleid NadiCare



Inhoudsopgave

Hoofdstuk 1 Inleiding	3
1.1 Bescherming van Persoonsgegevens	3
1.2 Contactgegevens	4
Hoofdstuk 2 Begripsbepalingen	5
Hoofdstuk 3 Toepassingsgebied	5
Hoofdstuk 4 Doel	6
Hoofdstuk 5 Vertegenwoordiging	6
Hoofdstuk 6 Voorwaarden voor rechtmatige verwerking	7
Hoofdstuk 7 Verwerking persoonsgegevens NadiCare en informeren van betrokkenen	7
Hoofdstuk 8 Verstrekken van persoonsgegevens aan derden	8
Hoofdstuk 9 Recht op inzage en afschrift van opgenomen persoonsgegevens	8
Hoofdstuk 10 Recht op aanvulling, correctie of verwijdering van opgenomen persoonsgegevens	8
Hoofdstuk 11 Beschikbaar stellen gegevens ECD	9
Hoofdstuk 12 Beveiliging	9
Hoofdstuk 13 Datalekken	11
13.1 Wanneer is er sprake van een datalek in de zorg?	11
13.2 Melden aan de Autoriteit Persoonsgegevens	11
13.3 Melden aan de betrokken personen	11
13.4 Maatregelen om datalekken in de zorg te voorkomen	11
Hoofdstuk 14 Klachten	13
Hoofdstuk 15 Wijzigingen, inwerkingtreding en inzage	13
Hoofdstuk 16 Bewaartermijnen van persoonsgegevens	14
16.1 Bewaartermijn voor cliëntgegevens	14
16.2 Bewaartermijn voor medewerkersgegevens	14
16.3 Wettelijk verplichte bewaartermijn	14
16.4 Verlengde bewaartermijnen	15
16.5 Veiligheid en vertrouwelijkheid	15
Hoofdstuk 17 Regeling taken en verantwoordelijkheden Functionaris voor Gegevensbescherming	16

Hoofdstuk 1 | Inleiding

De Algemene Verordening Gegevensbescherming (AVG), van kracht geworden op 25 mei 2018, legt strikte regels op ter bescherming van persoonsgegevens. Als zorgverlener is NadiCare zich bewust van de verantwoordelijkheid om de privacy van haar cliënten te waarborgen en heeft daarom dit privacyreglement opgesteld.

1.1 | Bescherming van Persoonsgegevens

1. Beschrijving van technische en organisatorische beveiligingsmaatregelen:

Om te voldoen aan de eisen van de AVG heeft NadiCare diverse technische en organisatorische maatregelen geïmplementeerd:

- Firewall: om ongeautoriseerde toegang tot het netwerk te voorkomen.
- Encryptie: voor het versleutelen van gegevens tijdens opslag en verzending.
- Toegangscontrole: om alleen geautoriseerd personeel toegang te verlenen tot gevoelige gegevens.
- Bewustzijnstraining: om personeel bewust te maken van hun verantwoordelijkheden.
- Incidentenbeheer en datalek melding: voor het adequaat reageren op en rapporteren van datalekken en andere beveiligingsincidenten.

2. Informatie over dataportabiliteitsverzoeken:

NadiCare biedt individuen het recht op dataportabiliteit, waardoor zij hun persoonsgegevens kunnen verkrijgen en overdragen aan een andere verwerkingsverantwoordelijke. Individuen kunnen een dataportabiliteitsverzoek indienen bij de functionaris voor gegevensbescherming (FG) van NadiCare, die binnen een vastgestelde termijn zal reageren om aan dit verzoek te voldoen.

Update van het reglement naar de laatste stand van de AVG:

NadiCare werkt voortdurend aan het bijwerken van haar privacyreglement naar de laatste stand van de AVG. Dit omvat het bepalen van relevante wijzigingen voor NadiCare, het doorvoeren van de nodige aanpassingen in definities en beschrijvingen van verwerkingsactiviteiten, en het toevoegen van nieuwe clausules om te zorgen voor volledige naleving van de AVG.

Het privacyreglement van NadiCare omvat:

- Uitleg over wettelijke vertegenwoordiging.
- Procedures voor de verwerking van persoonsgegevens, inclusief het verstrekken aan derden.
- Rechten van betrokkenen, zoals inzage, aanvulling, correctie of verwijdering van opgenomen persoonsgegevens.
- Beschikbaar stellen van gegevens in het Elektronisch Cliënten Dossier (ECD) en de rechten van cliënten hierbij.
- Beveiligingsmaatregelen ter bescherming van persoonsgegevens.

Procedures voor het omgaan met datalekken, inclusief melding aan de Autoriteit Persoonsgegevens en betrokken personen.

Dit privacyreglement is opgesteld om te voldoen aan de eisen van de AVG en om de privacy van cliënten te waarborgen. NadiCare blijft zich inzetten voor een veilige en vertrouwelijke verwerking van persoonsgegevens.

1.2 | Contactgegevens

Adres	: Hoofdstraat 40A
Postcode en Plaats	: 7901 JR Hoogeveen
Telefoon	: 06-42720279
Bestuurder	: Nadine Boorachi
Email	: info@nadicare.net
Website	: www.nadicare.net

Hoofdstuk 2 | Begripsbepalingen

- 2.1. **Persoonsgegevens:** alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare levende natuurlijke persoon. Losse gegevens die, wanneer samengevoegd, kunnen leiden tot de identificatie van een bepaalde persoon, worden ook beschouwd als persoonsgegevens. Zelfs wanneer de identiteitsgegevens zijn verwijderd, versleuteld of gepseudonimiseerd, maar ze nog steeds kunnen worden gebruikt om iemand opnieuw te identificeren, blijven ze persoonsgegevens en vallen ze binnen het toepassingsgebied van de AVG.
- 2.2. **Zorggegevens:** persoonsgegevens die direct of indirect betrekking hebben op de lichamelijke of geestelijke gesteldheid van betrokkene, verzameld door een beroepsbeoefenaar in het kader van zijn beroepsuitoefening. Dit geldt ook voor beroepsbeoefenaars in opleiding.
- 2.3. **Verwerking van persoonsgegevens:** elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
- 2.4. **Verstrekken van persoonsgegevens:** het bekend maken of ter beschikking stellen van gegevens.
- 2.5. **Verzamelen van persoonsgegevens:** het verkrijgen van persoonsgegevens.
- 2.6. **Dossier:** elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.
- 2.7. **Verantwoordelijke:** de natuurlijke persoon, rechtspersoon of het bestuursorgaan dat, alleen of samen met anderen, doel en middelen voor de verwerking van persoonsgegevens vaststelt.
- 2.8. **Bewerker:** degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
- 2.9. **Betrokkene:** degene op wie de persoonsgegevens betrekking hebben of zijn vertegenwoordiger.
- 2.10. **Derde:** ieder, niet zijnde de betrokkene, die gemachtigd is om persoonsgegevens te verwerken.
- 2.11. **Ontvanger:** degene aan wie de persoonsgegevens worden verstrekt (bijvoorbeeld bij een verwijzing).
- 2.12. **Toestemming van de betrokkene:** elke vrije, specifieke en op informatie berustende wilsuiting, waarmee de betrokkene aanvaardt dat op hem betrekking hebbende persoonsgegevens worden verwerkt.
- 2.13. **Het Autoriteit Persoonsgegevens:** De Autoriteit dat door de landelijke overheid is ingesteld om er op toe te zien dat de verwerking van persoonsgegevens conform de wet geschiedt.

Hoofdstuk 3 | Toepassingsgebied

Dit reglement is van toepassing op de verwerking van persoonsgegevens voor gerechtvaardigde doeleinden die in een dossier zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Het gaat zowel om persoonsgegevens die op papier staan als om elektronisch opgeslagen persoonsgegevens.

Hoofdstuk 4 | Doel

- 4.1. Het doel van dit reglement is om een praktische uitwerking te geven aan de bepalingen van de Algemene Verordening Gegevensbescherming, verder te noemen AVG;
- 4.2. Dit reglement is van toepassing binnen NadiCare en heeft betrekking op alle verwerkingen van persoonsgegevens van cliënten en medewerkers.

Hoofdstuk 5 | Vertegenwoordiging

Mensen met een ziekte of handicap of kinderen onder een bepaalde leeftijd zijn mogelijk niet in staat zijn om zelfstandig hun rechten uit te oefenen, in welk geval ruimte bestaat voor optreden door een vertegenwoordiger. De verantwoordelijke houdt zich bij de toepassing van de AVG aan de volgende aan de WGBO (Wet op de Geneeskundige behandelingsovereenkomst) ontleende regels:

- 5.1. Indien de betrokkene jonger is dan 12 jaar, treden de ouders of voogd, die het ouderlijk gezag uitoefenen, in de plaats van de betrokkene;
- 5.2. Dit geldt eveneens voor de betrokkene die de leeftijd van 12 jaar tot 18 jaar heeft en niet in staat kan worden geacht tot een redelijke waardering van zijn belangen;
- 5.3. Indien de betrokkene in de leeftijdscategorie van 12 tot 16 jaar valt en in staat is tot redelijke waardering van zijn belangen, treden naast de betrokkene zelf diens ouders of voogd op;
- 5.4. Een betrokkene van 16 jaar en ouder die in staat is tot een redelijke waardering van zijn belangen is geheel handelingsbekwaam en hoeft zich niet te laten vertegenwoordigen;
- 5.5. Indien de betrokkene ouder is dan 18 jaar en niet in staat kan worden geacht tot een redelijke waardering van zijn belangen ter zake, treedt in volgorde als hieronder weergegeven, als vertegenwoordiger op:
 - 5.6. De curator of mentor: indien betrokkene onder curatele staat of er ten behoeve van hem het mentorschap is ingesteld;
 - 5.7. De persoonlijk gemachtigde: indien betrokkene een bepaalde persoon schriftelijk gemachtigd heeft;
 - 5.8. Echtgenoot of levensgezel: indien de persoonlijk gemachtigde ontbreekt of niet optreedt;
 - 5.9. Een kind, broer of zus van betrokkene: indien de echtgenoot of levensgezel ontbreekt of niet wenst op te treden;
 - 5.10. De persoon die in de plaats treedt van de betrokkene, betracht de zorg van een goed vertegenwoordiger. Hij is gehouden de betrokkene zoveel mogelijk bij de vervulling van zijn taken te betrekken;
 - 5.11. Indien een vertegenwoordiger optreedt namens de betrokkene, komt de verantwoordelijke zijn verplichtingen die voortvloeien uit de wet en dit reglement na jegens deze vertegenwoordiger.

Hoofdstuk 6 | Voorwaarden voor rechtmatige verwerking

Teneinde de verwerking van persoonsgegevens van cliënten en medewerkers te voorzien van een rechtmatige basis zal NadiCare zich aan de volgende regels houden:

- 6.1. Persoonsgegevens worden in overeenstemming met dit reglement op behoorlijke en zorgvuldige wijze verwerkt (conform de AVG);
- 6.2. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (conform de AVG);
- 6.3. Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn (conform de AVG). Dit betekent dat de registratie van de persoonsgegevens moet passen binnen het voor die registratie omschreven doel, alsmede dat de aard en de omvang van de verzamelde gegevens dusdanig is, dat het doel van de registratie daarmee wordt bewerkstelligd;
- 6.4. De beheerder is verantwoordelijk voor het goed functioneren van de verwerking van persoonsgegevens. Zijn handelwijze met betrekking tot de verwerking van de persoonsgegevens en de verstrekking van gegevens wordt beperkt door dit reglement. De verantwoordelijke is aansprakelijk voor de eventuele schade als gevolg van het niet naleven van dit reglement;
- 6.5. De verantwoordelijke heeft de plicht ervoor zorg te dragen dat een niet aan zijn rechtstreeks gezag onderworpen bewerker van de persoonsgegevens zich contractueel gebonden weet aan dit reglement.

Hoofdstuk 7 | Verwerking persoonsgegevens NadiCare en informeren van betrokkenen

- 7.1. Persoonsgegevens betreffende iemands gezondheid, handicap of beperking mogen slechts worden verwerkt indien de betrokkene voor deze verwerking zijn ondubbelzinnige toestemming heeft verleend.

NadiCare maakt uitsluitend gebruik van persoonsgegevens waar de betrokkene toestemming voor heeft gegeven.

De verantwoordelijke informeert elke betrokkene die ingeschreven staat over de wijze waarop NadiCare met de persoonsgegevens omgaat. Voor uitwisseling van persoonsgegevens tussen medewerkers van NadiCare is geen expliciete toestemming van betrokkene vereist voor zover deze uitwisseling van belang is voor de uitvoering van de overeenkomst tussen betrokkene en NadiCare

Hoofdstuk 8 | Verstrekken van persoonsgegevens aan derden

- 8.1. Voor de verwerking van persoonsgegevens die bestaat uit het verstrekken van persoonsgegevens aan personen buiten NadiCare of aan andere instellingen is de toestemming van betrokkene vereist. Voor de gevallen waarin aan dit vereiste niet hoeft te voldaan volgt NadiCare de regeling in de WGBO (art. 7:457 BW). Dit betekent dat geen toestemming is vereist indien de verstrekking plaatsvindt op grond van een wettelijk voorschrift (lid 1), aan de vertegenwoordiger van de betrokkene of aan anderen die rechtstreeks zijn betrokken bij de uitvoering van de overeenkomst met betrokkene als bedoeld in lid 2 van art. 7:457 BW.

Hoofdstuk 9 | Recht op inzage en afschrift van opgenomen persoonsgegevens

- 9.1. De betrokkene heeft het recht kennis te nemen van de op zijn persoon betrekking hebbende verwerkte gegevens (recht op inzage);
- 9.2. De gevraagde inzage en/of het gevraagde afschrift zal zo spoedig mogelijk, doch uiterlijk binnen vier weken, plaatsvinden respectievelijk worden verstrekt;
- 9.3. Recht op inzage kan worden geweigerd of beperkt als het een onevenredig nadeel voor een derde met zich meebrengt (bijvoorbeeld wanneer zich in het dossier ook persoonsgegevens van familieleden bevinden). Een besluit tot weigering of beperking van inzage en afschrift wordt genomen door de directie van NadiCare .

Hoofdstuk 10 | Recht op aanvulling, correctie of verwijdering van opgenomen persoonsgegevens

- 10.1. Op uitdrukkelijk verzoek van de betrokkene worden de verzamelde persoonsgegevens aangevuld, gecorrigeerd, afgeschermd voor derden of verwijderd/vernietigd;
- 10.2. De betrokkene kan verzoeken om correctie van op hem betrekking hebbende gegevens indien deze feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift, in de verwerking voorkomen. Correcties moeten door NadiCare worden doorgegeven aan derden, indien zij de onjuiste gegevens hebben ontvangen;
- 10.3. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het schriftelijke verzoek tot aanvulling, correctie, afscherming of verwijdering/vernietiging in hoeverre hij daaraan wil voldoen. Niet gehonoreerde verzoeken worden schriftelijk gemotiveerd;
- 10.4. Een gehonoreerd verzoek tot verwijdering/vernietiging van gegevens wordt binnen drie maanden na honorering uitgevoerd.

Hoofdstuk 11 | Beschikbaar stellen gegevens ECD

- 11.1 NadiCare werkt met een Elektronisch Cliënten Dossier (ECD) voor haar cliënten zodat haar zorgverleners kunnen beschikken over actuele informatie betreffende hun cliënt.
- 11.2 De client geeft toestemming om in het ECD noodzakelijke informatie, zoals NAW, BSN, geboortedatum en medische relevante gegevens, die nodig zijn voor een goede zorgverlening beschikbaar te stellen en te delen met een daartoe bevoegde zorgprofessional van NadiCare of andere bij het zorgplan van cliënt betrokken zorgverleners zoals de huisarts of apotheker. Bepaalde zorgverleners, te weten bedrijfsarts, verzekeringsarts en keurend arts en ook verzekeraars hebben geen toegang tot het ECD.
- 11.3 De informatie wordt op een beveiligde versleutelde wijze digitaal beschikbaar gesteld. Alleen geautoriseerde zorgverleners kunnen gebruik maken van het ECD en informatie aanbieden en ophalen. Zorgverleners mogen alleen gegevens plaatsen en inzien van cliënten die behoren in het team van de desbetreffende zorgprofessional.
- 11.4 Volgens de Wet Aanvullende Bepalingen Verwerking Persoonsgegevens in de Zorg (Wabpvz), die wij volgen heeft de cliënt recht op/om:
- Kosteloze elektronische inzage in dossier, verwijfsindex en logging;
 - Afschrift uit dossier, verwijfsindex en logging
 - Kosteloos een elektronisch afschrift van het dossier te krijgen;
 - Het verzoeken om een overzicht van wie, wanneer bepaalde informatie beschikbaar heeft gemaakt en wie wanneer bepaalde informatie heeft ingezien (logging);
 - Gegevens aan het dossier toe te voegen voor wat betreft zelfmedicatie bij de apotheek;
 - Gegevens uit dossier of verwijfsindex te laten verwijderen/vernietigen;
 - Verzoeken tot vernietiging van gegevens bedoeld in artikel 7:454 BW en deze zullen dan binnen drie maanden na een daartoe strekkend verzoek van de cliënt vernietigd worden.

NadiCare verplicht zich hierbij om aan bovenstaande eisen te voldoen. Cliënt kan te allen tijde dit toestemmingsverklaring zonder opgaaf van reden intrekken.

Hoofdstuk 12 | Beveiliging

De AVG verplicht de verantwoordelijke technische- en organisatorische maatregelen te nemen om persoonsgegevens tegen onbevoegde inzage te beschermen. NadiCare heeft uitgebreide maatregelen geïmplementeerd om de veiligheid van persoonsgegevens te waarborgen:

- 12.1. Er worden niet meer persoonsgegevens verzameld dan nodig zijn voor het doel van de verzameling;
- 12.2. Alleen direct betrokken medewerkers hebben inzage in persoonsgegevens;
- 12.3. Alle persoonsgegevens zijn opgeborgen in afsluitbare kasten, laden, ruimten;
- 12.4. Elektronisch opgeslagen persoonsgegevens zijn alleen na ingeven van een persoonlijk wachtwoord in te zien;
- 12.5. Elektronisch opgeslagen gegevens worden versleuteld verzonden, zowel via internet als via andere dragers.;

- 12.6. Medewerkers hebben een geheimhoudingsplicht betreffende persoonsgegevens. In dit kader wordt onder de term 'medewerkers' eveneens begrepen: invalkrachten en stagiaires. Hierbij geldt de aanvullende bepaling dat op de verantwoordelijke de verantwoordelijkheid rust deze categorie medewerkers expliciet en nadrukkelijk bekend te maken met het van kracht zijn van dit reglement.
- 12.6. NadiCare heeft technische maatregelen genomen om de integriteit en vertrouwelijkheid van persoonsgegevens te waarborgen. Deze maatregelen omvatten het gebruik van geavanceerde encryptietechnologieën tijdens gegevensoverdracht en opslag, zowel intern als extern. Alle elektronisch opgeslagen persoonsgegevens worden versleuteld verzonden, waardoor ongeoorloofde toegang tot de gegevens wordt voorkomen.
- 12.7. Daarnaast hanteert NadiCare strikte toegangscontrolemaatregelen om alleen geautoriseerd personeel toegang te verlenen tot gevoelige gegevens. Personeel krijgt specifieke toegangsrechten toegewezen op basis van hun functie en verantwoordelijkheden, en deze rechten worden regelmatig gecontroleerd en bijgewerkt volgens de vereisten van de organisatie.
- 12.8. Bovendien heeft NadiCare procedures geïmplementeerd voor pseudonimisering, wat inhoudt dat persoonsgegevens zodanig worden verwerkt dat ze niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder het gebruik van aanvullende informatie. Dit draagt bij aan een verdere bescherming van de privacy van onze cliënten.

De combinatie van deze technische en organisatorische maatregelen stelt NadiCare in staat om op een effectieve wijze te voldoen aan de eisen van de AVG en de privacy van onze cliënten te waarborgen.

Hoofdstuk 13 | Datalekken

Vanaf 1 januari 2016 is de meldplicht datalekken van kracht. Deze meldplicht houdt in dat zorgorganisaties een datalek van persoonsgegevens verplicht moeten melden aan de Autoriteit Persoonsgegevens en in sommige gevallen ook aan de betrokken personen.

13.1 | Wanneer is er sprake van een datalek in de zorg?

Wat is een datalek? Bij een datalek vallen gegevens (data) in handen van derden die daar geen toegang toe zouden mogen hebben. Een datalek is het gevolg van een probleem in de beveiliging. Meestal gaat het om digitale gegevens maar het kan natuurlijk ook gaan om een medisch dossier dat uit de kast wordt gestolen of een printje met daarop patiëntengegevens dat iemand verliest. Een datalek kan ontstaan als er een USB-stick op straat komt te liggen, het systeem gehackt wordt en ook als er per ongeluk persoonsgegevens gewist worden zonder dat daar een back-up van beschikbaar is.

13.2 | Melden aan de Autoriteit Persoonsgegevens

Wanneer er sprake is van een datalek maakt NadiCare vervolgens een afweging of daarvan een melding gemaakt moet worden bij de Autoriteit Persoonsgegevens. Allereerst kijkt NadiCare of er sprake is van een datalek van persoonsgegevens. Wanneer het alleen om gegevens van de organisatie gaat hoeft er namelijk niet gemeld te worden. Bij persoonsgegevens moet er sprake zijn van een kans op nadelige gevolgen voor de bescherming van deze persoonsgegevens. Als dat het geval is kijkt NadiCare nog om wat voor soort gegevens het gaat. Er moet een melding gemaakt worden als er sprake is van veel gegevens en/of er sprake is van gevoelige informatie. Bijvoorbeeld data over iemands geloof, financiële gegevens, medische gegevens, psychologische gegevens, wachtwoorden en gegevens die gebruikt kunnen worden voor identiteitsfraude (zoals biometrische gegevens, BSN- nummer). Melden bij de Autoriteit Persoonsgegevens moet binnen 72 uur!

13.3 | Melden aan de betrokken personen

NadiCare maakt een aparte afweging voor het melden aan de betrokken personen. Wanneer er melding gedaan wordt aan de betrokken personen moet er ook altijd een melding doen aan de Autoriteit Persoonsgegevens. Een melding aan de betrokken personen is nodig als er misbruik gemaakt kan worden van de gegevens. Bijvoorbeeld wanneer medische gegevens van een beroemd persoon gelekt zijn en deze mogelijk gepubliceerd zullen worden. De persoon kan zich hier dan goed op voorbereiden en eventueel maatregelen nemen. NadiCare meldt dit dan ook zo snel mogelijk!

13.4 | Maatregelen om datalekken in de zorg te voorkomen

- ✓ Een goede beveiliging van gevoelige gegevens door versleuteling (encryptie). Daarmee wordt voorkomen dat er gegevens na een lek te herleiden zijn tot een persoon.
- ✓ Voorkomen dat medewerkers persoonsgegevens verspreiden via de e-mail en/of Clouddiensten waar geen contract mee is afgesloten zoals Dropbox.
- ✓ Medewerkers geïnformeerd die met persoonsgegevens omgaan over de meldplicht persoonsgegevens.

- ✓ NadiCare heeft afspraken over voorkomen datalek met andere organisaties waarmee wordt samengewerkt en persoonsgegevens worden uitgewisseld.
- ✓ Werkwijze melden datalek:

De verantwoordelijke om het datalek te melden aan de Autoriteit Persoonsgegevens is de FG. De Autoriteit Persoonsgegevens stelt voor de melding een webformulier beschikbaar (<https://datalekken.autoriteitpersoonsgegevens.nl>). Het datalek wordt onverwijld gemeld. Dit houdt in dat de FG, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen. De termijn voor het melden begint te lopen op het moment dat de FG of een bewerker op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt. Zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, zal een melding worden gedaan, tenzij op dat moment inmiddels uit onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt.

- ✓ Het datalek hoeft niet te worden gemeld aan de betrokkene indien één van de volgende situaties zich voordoet:

Er zijn passende technische beschermingsmaatregelen genomen waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, bijvoorbeeld door adequate encryptie (versleuteling) en hashing (het omzetten van gegevens in een unieke code);

Andere technische beschermingsmaatregelen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten, bijvoorbeeld door een tijdige en adequate remote wiping (het op afstand wissen van de gegevens die op een apparaat staan) en pseudonimisering (technische maatregelen om te voorkomen dat de persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene);

Het is onwaarschijnlijk dat het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene: als persoonsgegevens van gevoelige aard zijn gelekt, moet sowieso worden gemeld;

Er zijn andere zwaarwegende redenen om de melding aan de betrokkene achterwege te laten.

- ✓ Als het datalek wel wordt gemeld aan betrokkene dan zal in de kennisgeving aan de betrokkene in ieder geval worden vermeld:
 - De aard van de inbreuk,
 - De instanties waar de betrokkene meer informatie over de inbreuk kan krijgen (contactgegevens) en
 - De maatregelen die zijn aanbevolen om de negatieve gevolgen van de inbreuk te beperken.
- ✓ Vastlegging gegevens: Er zal een register worden bijgehouden van alle datalekken die onder de meldplicht vallen, dus datalekken die aan de Autoriteit Persoonsgegevens moeten worden gemeld. Per datalek bevat het register in ieder geval de gegevens omtrent de aard van de inbreuk en, indien aan de betrokkene is gemeld, de tekst van de kennisgeving. De bewaartermijn hiervan is minimaal drie jaar.

Hoofdstuk 14 | Klachten

Indien de betrokkene van mening is dat de bepalingen van dit reglement niet worden nageleefd of andere reden heeft tot klagen, kan hij zich wenden tot:

- 14.1. De verantwoordelijke;
- 14.2. De leidinggevende van de verantwoordelijke, waarbij de interne klachtenregeling van NadiCare van toepassing is;
- 14.3. Het Autoriteit Persoonsgegevens, met een verzoek een onderzoek in te stellen of de wijze van gegevensverwerking door de verantwoordelijke in overeenstemming is met de Wet bescherming persoonsgegevens, dan wel gebruik te maken van de AVG neergelegde beroepsmogelijkheden.

Hoofdstuk 15 | Wijzigingen, inwerkingtreding en inzage

- 15.1 Wijzigingen van het reglement worden aangebracht door verantwoordelijke;
- 15.2 De wijzigingen in het reglement zijn van kracht vier weken nadat ze bekend zijn gemaakt aan betrokkenen;
- 15.3 Dit reglement is van kracht per bestuursbesluit en bij de verantwoordelijke in te zien;

Hoofdstuk 16 | Bewaartermijnen van persoonsgegevens

NadiCare streeft naar volledige naleving van alle wettelijke vereisten met betrekking tot gegevensbeheer, inclusief het vaststellen en handhaven van bewaartermijnen voor persoonsgegevens. Deze bewaartermijnen zijn duidelijk gecommuniceerd naar onze cliënten, personeelsleden en vrijwilligers. Indien iemand om welke reden dan ook wil afwijken van deze termijnen, staat het hen vrij om dit aan te geven. We verzekeren dat dergelijke verzoeken zorgvuldig worden behandeld, met volledige inachtneming van de geldende wet- en regelgeving.

16.1 | Bewaartermijn voor cliëntgegevens

Persoonsgegevens van cliënten worden bewaard gedurende de periode dat zij zorg ontvangen van NadiCare, vermeerderd met een wettelijk vastgestelde maximumtermijn van 15 jaar na de beëindiging van de zorgrelatie, tenzij een langere bewaartermijn wettelijk vereist is. Deze termijn is afgeleid van de Wet Geneeskundige Behandelingsovereenkomst (WGBO), die voorschrijft dat medische dossiers 15 jaar moeten worden bewaard na de beëindiging van de behandeling.

Het dossier omvat verschillende documenten, waaronder het zorgplan, de zorgverleningsovereenkomst, verwijzingen van het zorgkantoor, indicatiebesluiten, verslagen van de medische voorgeschiedenis, actuele medische gegevens en mutaties in de zorgverlening.

16.2 | Bewaartermijn voor medewerkersgegevens

De persoonsgegevens van medewerkers worden bewaard gedurende hun dienstverband bij NadiCare en tot 2 jaar na beëindiging van hun dienstverband, tenzij een langere bewaartermijn wettelijk vereist is.

16.3 | Wettelijk verplichte bewaartermijn

Er gelden specifieke bewaartermijnen voor verschillende documenten en personeelsgegevens:

- Sollicitatiebrieven en -correspondentie mogen maximaal vier weken na de sollicitatieprocedure worden bewaard, tenzij expliciete toestemming van de sollicitant wordt verkregen voor toekomstige vacatures.
- Verslagen van functioneringsgesprekken moeten minimaal twee jaar worden bewaard na het vertrek van een medewerker. Loonbelastingverklaringen en kopieën van identiteitsbewijzen moeten minimaal vijf jaar worden bewaard, terwijl afspraken over salaris en arbeidsvoorwaarden minimaal zeven jaar geldig zijn. Voor specifieke documenten zoals arbeidsovereenkomsten en verslagen in het kader van de Wet verbetering poortwachter geldt een maximale bewaartermijn van twee jaar.
- Financiële gegevens en administratieve documenten waar persoonsgegevens in voorkomen, zoals facturen, contracten en correspondentie, dienen volgens de fiscale bewaarplicht 7 jaar te worden bewaard.

16.4 | Verlengde bewaartermijnen

In gevallen waarin een langere bewaartermijn wettelijk is voorgeschreven of nodig is voor juridische procedures, kunnen persoonsgegevens langer worden bewaard.

16.5 | Veiligheid en vertrouwelijkheid

Na het verstrijken van de bewaartermijn zullen de persoonsgegevens op een veilige en vertrouwelijke wijze worden vernietigd of geanonimiseerd, tenzij er een rechtmatig belang bestaat om de gegevens te bewaren. Dit kan onder meer vereist zijn voor juridische doeleinden, naleving van wettelijke verplichtingen, archivering in het algemeen belang, wetenschappelijk onderzoek of statistische doeleinden, waarbij NadiCare ervoor zal zorgen dat de gegevens adequaat worden beschermd.

Hoofdstuk 17 | Regeling taken en verantwoordelijkheden functionaris voor Gegevensbescherming

Artikel 1: definities

- a. AVG: Algemene Verordening Gegevensbescherming;
- b. FG: functionaris voor gegevensbescherming artikel 37 van de AVG;
- c. Beheerder: het bestuur van NadiCare .
- d. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, bedrijf, organisatie, een dienst of een ander orgaan die/dat ten behoeve van de beheerder persoonsgegevens verwerkt;
- e. Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (betrokkene) waarbij als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
- f. Verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
- g. Personeel: medewerkers in loondienst en/of extern ingehuurd medewerkers die in opdracht van de beheerder werkzaamheden verrichten.

Artikel 2: Taken

- 1. De FG heeft de volgende taken:
 - a. het houden van toezicht op verwerkingen van persoonsgegevens;
 - b. toezicht op wijzigingen in bestaande verwerkingen en/of het aanleggen van nieuwe verwerkingen met persoonsgegevens binnen NadiCare ;
 - c. overleg met de contactpersoon van de Autoriteit Persoonsgegevens;
 - d. Organiseren, inrichten en/of onderhouden van het verwerkingsregister met alle verwerkingen persoonsgegevens binnen NadiCare ;
 - e. het (laten) afhandelen van klachten inzake privacy;
 - f. Overige door het bestuur of directie van NadiCare aan de FG opgedragen werkzaamheden aangaande privacy.
- 2. Het personeel meldt bij de FG alle (nieuwe) verwerkingen van persoonsgegevens alsmede eventuele incidenten met betrekking tot privacy.

Artikel 3: Bevoegdheden

1. De FG is bevoegd, zo nodig met medeneming van de benodigde apparatuur, elke plaats in de gebouwen op de terreinen die bij NadiCare in gebruik zijn en waar persoonsgegevens worden verwerkt, te betreden.
2. De FG is bevoegd inlichtingen te vorderen van een ieder die onder gezag of in opdracht van NadiCare werkzaam is of overeenkomstig voor of namens NadiCare persoonsgegevens verwerkt.
3. De FG is bevoegd inzage te vorderen van zakelijke gegevens en bescheiden waarin persoonsgegevens zijn verwerkt.
4. De FG is bevoegd van de gegevens en bescheiden kopieën te maken.
5. Indien het maken van kopieën niet ter plekke kan gebeuren, is hij bevoegd de gegevens en bescheiden voor maximaal één werkdag mee te nemen.
6. De FG is bevoegd tot het geven van een opdracht tot
 - a. het aanmaken van een registratie van persoonsgegevens in overeenstemming met de AVG;
 - b. vernietiging van persoonsgegevens, waarvan de bewaartermijn is overschreden of indien de gegevensverwerking onrechtmatig is.
7. De FG is bevoegd zich te laten vergezellen en bijstaan door personen die daartoe door hem zijn aangewezen.
8. De FG maakt van de bevoegdheden als bedoeld in dit artikelen slechts gebruik voor zover dit redelijkerwijs voor de uitoefening van de taak noodzakelijk is.

Artikel 4: Weigering

1. Een ieder, die werkzaam is bij en/of in opdracht werkt van de verantwoordelijke, is verplicht aan de FG medewerking te verlenen, die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden.
2. Indien de medewerking aan de uitoefening van de bevoegdheden van de FG zoals bedoeld in artikel 3, wordt geweigerd, kan NadiCare, op een met redenen omkleed verzoek, toestemming verlenen aan de FG de benodigde handelingen zelfstandig uit te voeren in weerwil van de weigering tot medewerking.
3. Het bestuur en/of directie van NadiCare wordt zo spoedig mogelijk in kennis gesteld over de uitvoering van het bepaalde in dit artikel.

Artikel 5: Geheimhouding

1. De FG is verplicht tot geheimhouding van al hetgeen hem op grond van deze regeling bekend is geworden, tenzij de betrokkene in bekendmaking toestemt.

Artikel 6: Regeling

1. Deze regeling wordt vastgesteld en gewijzigd bij besluit van de beheerder.
2. Deze regeling zal intern aan cliënten en personeel bekend worden gemaakt door publicatie op de website www.nadicare.net.