Privacy beleid Stichting Rooz

Algemene Verordening Gegevensbescherming

25 mei 2018

STICHTING ROOZ

Inhoudsopgave privacybeleid Stichting ROOZ

Algemeen

Beleidsonderwerpen:

Bijlagen:

1. Aanleiding

Stichting ROOZ vindt het belangrijk privacy te waarborgen voor hun cliënten en medewerkers. Privacy is een ruim begrip: het gaat onder meer om de bescherming van persoonsgegevens maar ook om de bescherming van het eigen lichaam en de woon- en leefomgeving van de cliënt. Ook bij het rapporteren over cliënten dient rekening te worden gehouden met de privacygevoelige informatie. Hierbij kan gedacht worden aan werknotities, zorgdossiers, rapportage via email en telefoon.

In het kader van de Algemene Verordening gegevensbescherming (AVG) en de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO) is iedere instelling die werkzaam is binnen de gezondheidszorg verplicht om een privacybeleid te hebben. Om de privacy van al deze betrokkenen te beschermen is het van groot belang dat de verwerking van persoonsgegevens zorgvuldig gebeurt en dat hierbij wordt voldaan aan de wet- en regelgeving die wij op het gebied van de bescherming van persoonsgegevens in Nederland kennen.

Dit privacybeleid is verdeeld in twee delen. In het eerste deel worden de randvoorwaarden beschreven voor het in het tweede deel beschreven beleid voor de bescherming van persoonsgegevens.

Om de privacy van zowel de cliënt als de medewerker te waarborgen is beleid vastgelegd.

Het privacybeleid is geschreven conform:
- De AVG (Algemene Verordening Gegevensbescherming)
- De Wet geneeskundige Behandelingsovereenkomst (WGBO)
- De geheimhoudingsplicht werknemer vastgelegd in arbeidscontract.
- De privacy voorwaarden conform contract met de Foodvalley

Dit document wordt gebruikt door alle medewerkers van Stichting ROOZ.

Verantwoordelijkheden:
De verantwoordelijkheden ten aanzien van het privacybeleid zijn als volgt verdeeld:
De Raad van Bestuur is verantwoordelijk voor het vaststellen van het privacybeleid en het reglement. Daarnaast is de Raad van Bestuur verantwoordelijk voor het implementeren en onderhouden van het privacybeleid. Alle medewerkers zijn persoonlijk verantwoordelijk voor het handhaven van het privacybeleid. De medewerker dient contact op te nemen met de Raad van Bestuur, wanneer de medewerker van mening is dat het individueel belang van een cliënt of diens familie zwaarder weegt dan het privacybelang.

Algemeen

2. Begrippen

In dit hoofdstuk wordt nadere uitleg gegeven over een aantal begrippen die in het privacybeleid voorkomen en worden de uitgangspunten beschreven die betrekking hebben op het beleid omtrent de bescherming van persoonsgegevens binnen Stichting ROOZ.

De algemene omschrijving van de begrippen sluit aan bij de definities in de AVG (Artikel 4).

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Identificeerbaar wil zeggen direct- of indirect identificeerbaar aan de hand van bijvoorbeeld een naam, nummer, of locatiegegevens (identificatoren, al dan niet online) of aan de hand van een aantal elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van de betreffende natuurlijke persoon.

Betrokkene
Een betrokkene is degene op wie een persoonsgegeven betrekking heeft. Bijvoorbeeld de verwerkingen van gegevens van cliënten van Stichting ROOZ, derden informatie verstrekking zorginstanties/gemeenten, medewerkers van Stichting ROOZ, etc.

Verwerkingsverantwoordelijke
De natuurlijke persoon of rechtspersoon die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Dit is Stichting ROOZ.

Verwerker
Een verwerker is degene die ten behoeve van de verwerking verantwoordelijke persoonsgegevens verwerkt. Bij een verwerker gaat het altijd om een persoon of organisatie buiten Stichting ROOZ.

Toestemming van de betrokkene
Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting, waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.

Verwerken van persoonsgegevens
Dit is in feite elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés. Deze handelingen kunnen bestaan uit verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden, of op een andere wijze ter beschikking stellen, aligneren, combineren, afschermen wissen, of vernietigen.

Functionaris voor gegevensbescherming

Stichting ROOZ moet onder de AVG een Functionaris voor gegevensbescherming (FG) aanstellen (artikel 37/38/39 AVG). Zie functieomschrijving FG bijlage 2

De FG ondersteunt de medewerkers van Stichting ROOZ bij het opereren binnen de wettelijke kaders en de binnen Stichting ROOZ gemaakte afspraken en zorgt er voor dat privacy-aangelegenheden uniform en gecoördineerd worden opgepakt.

De FG heeft de (vanuit de RvB gedelegeerde) verantwoordelijkheid om een privacybeleid op te stellen, te coördineren en te monitoren. Dit geldt eveneens voor de taken die vanuit het beleid op centraal niveau moeten worden uitgevoerd. De RvB stelt het beleid, kaders en normen vast.
De divisies hebben de (gedelegeerde) verantwoordelijkheid voor de uitvoering van dit Privacybeleid.

Juridisch Zwitsers zakmes

Deze wordt gehanteerd bij het transparantiebeginsel;
- minst ingrijpende maatregel kiezen
- verhouding tussen maatregel en doel goed afwegen
- meest geschikte maatregel nemen

Beleidsonderwerpen

3. Verwerkingsregister

Conform Artikel 30 lid 1 AVG dient de verwerkingsverantwoordelijke een register bij te houden met verwerkingsactiviteiten. Dit mag schriftelijk en/of elektronisch.

- Zie voor verwerkingsregister google drive -> kwaliteitsmanagement -> AVG
- Zie bijlage 1 procedure verwerkingsregister

In dit register staat het volgende gedocumenteerd:

- ➢ welke categorie persoonsgegevens u verwerkt, bijvoorbeeld medische gegevens,
- ➢ met welk doel u dit doet, bijvoorbeeld behandeling van de patiënt of het opstellen van een factuur,
- ➢ wie de gegevens aan u heeft gegeven, bijvoorbeeld cliënten of andere zorgverleners,
- ➢ met wie u de gegevens deelt, bijvoorbeeld andere zorgverleners.

Het verwerkingsregister kan opgevraagd worden door de Autoriteit Persoonsgegevens.
Een verwerking kan uit één of meer handelingen bestaan. Verwerkingsactiviteiten die in het maatschappelijk verkeer als een eenheid worden beschouwd, worden gezien als één gegevensverwerking, bijvoorbeeld een cliëntenadministratie.

4. Transparantie en informatieplicht

In art. 5 AVG is het transparantiebeginsel opgenomen. In artikel 13 en 14 AVG staat de informatie die verstrekt moet worden aan betrokkenen.

Transparantie is een van de belangrijkste verplichtingen als persoonsgegevens verwerkt worden. Om de betrokkene in staat te stellen zijn rechten te verwezenlijken, moet hij van de verwerking van hem betreffende gegevens op de hoogte zijn. Het niet voldoen aan de informatieplicht leidt, tenzij er een wettelijke uitzondering is, tot een onrechtmatige verwerking van persoonsgegevens. Transparant zijn in wat Stichting ROOZ doet met gegevens en de verplichte informatie verstrekken aan betrokkenen staat daarom voorop.

De cliënt wordt zo spoedig als mogelijk geïnformeerd over het voornemen tot verwerking van op hem betrekking hebbende persoonsgegevens. Cliënten worden op zodanige wijze als past bij zijn bevattingsvermogen ingelicht over het doel van de gegevensverwerking, met wie zijn gegevens zullen worden gedeeld en welke belang daarbij voor hem aanwezig is. Dit zal in het intakeproces aan de orde komen. Tevens wordt de cliënt geïnformeerd over de identiteit van de professional die de verwerking doet. Op verzoek van de cliënt worden deze gegevens schriftelijk verstrekt. De cliënt heeft de mogelijkheid bezwaar te maken tegen de verwerking van diens gegevens. Indien en voor zover de betrokkene van dit recht gebruik maakt, wordt - in overleg met cliënt - diens bezwaren besproken en gewogen. Beoordeeld wordt het gewicht van de bezwaren van de cliënt ten opzichte van het doel en de noodzaak om wél gegevens te verwerken. Afhankelijk van de uitkomst van dit weegproces worden de bezwaren (tijdelijk) gehonoreerd of terzijde geschoven. Het voornemen om de bezwaren van de cliënt terzijde te schuiven, wordt eerst getoetst met het 'juridisch Zwitsers zakmes'. De argumenten op basis waarvan bezwaren terzijde worden geschoven, worden zorgvuldig gemotiveerd en gedocumenteerd.

Het recht op informatie kan (tijdelijk) worden beperkt voor zover dit noodzakelijk is ter voorkoming van strafbare feiten, indien in het belang van de bescherming van de cliënt of in belang van de rechten en vrijheden van anderen. Het besluit om het recht op informatie te beperken, dient te worden getoetst met het 'juridisch Zwitsers zakmes'. De argumenten op basis waarvan het recht op informatie wordt beperkt, worden zorgvuldig gemotiveerd en gedocumenteerd.

De cliënt dient altijd schriftelijk toestemming te verlenen om andere personen dan bij punt 1 beschreven inzage te geven in cliëntgegevens. Dit ondervangt Stichting ROOZ door de cliënt te laten ondertekenen voor inloggegevens van het digitaal cliëntdossier of door het format 'Toestemming uitwisselen informatie met derden' in te laten vullen/tekenen.

Informatie verzamelen en opslaan, cliënt geeft toestemming bij ondertekenen van intakeformulier

Informatie delen;

- Toestemming uitwisselen informatie met derden
- Toestemmingsformulier VTG
- Toestemmingsverklaring P&O uitwisseling gegevens derden

5. Doelen en Doelbinding / Verenigbaar gebruik

Een doel / doelen voor verzameling van Persoonsgegevens moeten voldoen aan de volgende eisen:

- ➢ Welbepaald;
- ➢ Uitdrukkelijk omschreven; en,
- ➢ Gerechtvaardigd.
- ➢ Een doel moet omschreven zijn vóórdat de verzameling van gegevens plaatsvindt

5.1 Noodzakelijkheidstoets

Vervolgens mogen persoonsgegevens niet verder op een met de verzamel doeleinden onverenigbare wijze worden verwerkt (doelbinding / verenigbaar gebruik) (art. 5 lid 1 sub b AVG). Persoonsgegevens moeten toereikend zijn, ter zake dienen en beperkt tot wat noodzakelijk is voor het doel (minimale gegevensverwerking art. 5 lid 1 sub c AVG). Kortom, niet teveel en niet te weinig. De vraag die altijd gesteld dient te worden als het doel bepaald is: Welke gegevens zijn noodzakelijk voor het doel?

Bij het inrichten van de gegevensverwerking moet steeds nagegaan worden of het verwerken van persoonsgegevens noodzakelijk is voor het doel. Vraag is of met minder gegevens hetzelfde doel bereikt kan worden of dat door het treffen van (technische) maatregelen er minder persoonsgegevens verwerkt hoeven worden. Als dat zo is, moet de verwerking daar op aangepast worden.

Als gegevens niet meer nodig zijn voor het behalen van een doel dan moeten deze worden verwijderd (dan wel niet meer gebruikt voor dat doel als ze nog andere doelen dienen waarvoor de gegevens wel voor bewaard moeten blijven). In overeenstemming met dat principe, moet Stichting ROOZ specificeren hoe lang persoonsgegevens gebruikt / bewaard mogen worden voor een specifieke doel.

- Zie DPIA voor bewaartermijnen

6. Rechtmatige grondslag

Rechtsgrondslagen snelweg Toestemming als vluchtstrook					
< noodzakelijkheid >					
6.1.a Toestemming	6.1.b Aangaan of uitvoeren overeenkomst	6.1.c Wettelijke plicht	6.1.d Vitaal belang	6.1.e Publieke taak	6.1.f Rechtvaardig belang
intrekken				bezwaar	bezwaar

De verwerking van persoonsgegevens moet gebaseerd zijn op één van de zes in de AVG limitatief genoemde grondslagen (art. 6 AVG).

De volgende grondslagen zijn van toepassing voor Stichting ROOZ.

- **6.1.a Toestemming van ouders/verzorgers voor het verwerken van bijzondere gegevens met als doel het bieden van zorg**
- **6.1.b Ondertekening van het zorgplan en evaluaties en raamovereenkomsten met gemeenten**
- **6.1.c Het is noodzakelijk om gegevens te verwerken over cliënten en personeel**
- **6.1.f Het is noodzakelijk om gegevens te verwerken over cliënten**

Toelichting op de grondslagen zoals hierboven genoemd;

6.1.a U mag iemand niet onder druk zetten om toestemming te geven. Er moet sprake zijn van actieve handeling (schriftelijke of mondelinge verklaring). Toestemming moet steeds gelden voor een specifiek doel, toestemming moet net zo makkelijk in te trekken zijn als dat het was om deze te geven en u moet kunnen aantonen dat u geldige toestemming heeft verkregen.
Verplicht informeren over:
- Identiteit van de organisatie;
- Doel verwerking;
- Welke persoonsgegevens u verzamelt en gebruikt;
- Het recht dat zij hebben om de toestemming weer in te trekken.

Voldoet de toestemming niet aan deze eisen? Dan is de toestemming niet geldig. U mag de persoonsgegevens dan niet verwerken. De AVG geeft kinderen jonger dan 16 jaar extra bescherming. Want kinderen kunnen de risico's van een gegevensverwerking niet of minder goed inschatten. Daarom moeten zij toestemming hebben van de persoon die de ouderlijke verantwoordelijkheid draagt.

6.1.b U mag zich op deze grondslag baseren als u een overeenkomst heeft met iemand en hiervoor het verwerken van persoonsgegevens noodzakelijk is. De overeenkomst zelf mag niet gericht zijn op het verwerken van persoonsgegevens, maar moet een ander doel hebben.

6.1.c De verwerking van de persoonsgegevens dient noodzakelijk te zijn om aan een wettelijke verplichting te voldoen. Het hoeft niet expliciet in de wet te staan dat u voor de uitvoering van een specifieke taak persoonsgegevens moet verwerken. Soms is de verplichting in de wet namelijk ruimer

geformuleerd. Het is dan aan u om te bepalen of het verwerken van persoonsgegevens noodzakelijk is om aan uw verplichting te voldoen.

6.1.d Een vitaal belang is aan de orde als het over een belang gaat dat essentieel is voor iemands leven of gezondheid en u die persoon niet om toestemming kunt vragen. Bijvoorbeeld wanneer er acuut gevaar dreigt maar iemand bewusteloos is of mentaal niet in staat is om toestemming te geven.

6.1.e U kunt zich alleen op deze grondslag beroepen als u een publieke taak uitoefent voor het algemeen belang of openbaar gezag. Het gaat daarbij om taken die in de wet zijn vastgelegd en die relevant zijn voor uw organisatie. Het moet voor mensen ook duidelijk zijn dat u hun persoonsgegevens verwerkt voor de uitoefening van die specifieke wettelijke taak. Daarnaast moet de verwerking van de persoonsgegevens noodzakelijk zijn om uw publieke taak goed te kunnen vervullen. Bijvoorbeeld: u zet als gemeente cameratoezicht in op openbare plaatsen voor de openbare veiligheid.

6.1.f U kunt zich op deze grondslag baseren als u aan drie voorwaarden voldoet:
(1) u heeft een gerechtvaardigd belang, bijvoorbeeld het voeren van een personeelsadministratie
(2) de verwerking is noodzakelijk om dit gerechtvaardigde belang te behartigen, u moet de verwerking toetsen aan de eisen van 1. proportionaliteit en 2. subsidiariteit. Dat betekent dat u moet nagaan of 1. het doel van de verwerking in verhouding staat tot de inbreuk voor de personen van wie u persoonsgegevens verwerkt en 2. of u het doel niet op een voor de betrokken personen minder nadelige manier kan bereiken.
(3) u heeft een afweging gemaakt tussen uw belangen en die van de personen van wie u persoonsgegevens verwerkt.

Is geen van deze grondslagen aanwezig, dan is de verwerking van persoonsgegevens niet toegestaan. Het is belangrijk om de verwerkingsgrondslag vast te stellen, omdat de verwerking daar op ingericht moet worden. De verplichtingen als verantwoordelijke en de rechten van de betrokkene kunnen namelijk verschillen afhankelijk van de verwerkingsgrondslag.

6.2 Toestemming (Art. 6 lid 1 sub a AVG)
Onder de AVG worden strenge eisen gesteld aan het verkrijgen van een geldige toestemming als grond voor de gegevensverwerking (strenger dan onder de Wbp).
Toestemming: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting daarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt. (art 4 lid 11 AVG).

- Vrije wil: Een daadwerkelijke keuze voor de betrokkene.
- Specifiek: een goed gedefinieerd concreet doel waarvoor toestemming wordt gegeven Dat betekent dat de verschillende doelen waarvoor toestemming wordt gevraagd bijvoorbeeld gespecificeerd worden en dat een cliënt ook per doel ja/nee kan aangeven.
- Geïnformeerd: De betrokkenen moet vóór het geven van de toestemming zo geïnformeerd zijn dat hij begrijpt wat de betrokken gegevens zijn, waarvoor hij toestemming geeft en wat de implicaties daarvan zijn.
- Ondubbelzinnig: Er mag geen twijfel zijn over de (inhoud en reikwijdte van de) toestemming.

Aanvullende eisen uit de AVG:

- De verantwoordelijke moet toestemming kunnen aantonen (art. 7 lid 1 AVG)
- De toestemming moet zijn opgesteld in begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal (art. 7 lid 2 en art 12 lid 1 AVG).
- Het intrekken van de toestemming moet net zo makkelijk zijn als het geven er van (art 7 lid 3 AVG).
- De grondslag toestemming kan in principe niet worden gebruikt voor gegevens die niet noodzakelijk zijn voor de uitvoering van een overeenkomst, maar waarvoor de betrokkene wel toestemming geeft door het aangaan van de overeenkomst. De ''vrije wil'' staat dan ter discussie (art. 7 lid 4 AVG)
- Als er meerdere doelen zijn, moet toestemming voor elk daarvan worden verkregen (Overweging 32 AVG).
- Bij toestemming d.m.v. een schriftelijke verklaring (zoals een overeenkomst) moeten doelen waarvoor toestemming gevraagd wordt los van elkaar en separaat van andere informatie gepresenteerd worden (anders is een deel van de overeenkomst niet bindend) (art 7 lid 2 AVG).
- Bij minderjarigen moet de verantwoordelijke verifiëren of de toestemming is gegeven of geautoriseerd door de ouder (art. 8 AVG)
- Een verzoek om toestemming via elektronische middelen dient duidelijk, transparant en beknopt te zijn (Art 12 lid 1 AVG).

<u>Informatie delen financierende partij</u>:
Om onze zorg uit te kunnen voeren, hebben wij een verantwoordingsplicht aan de financierende partij. De financierende partij is de gemeente. In het belang van de zorg de cliënt is het belangrijk dat informatie wordt gedeeld over de voortgang en de behaalde doelen. Hiervoor zullen indien nodig de evaluatieverslagen met de financierende partij gedeeld worden. Middels ondertekening van het intakeformulier, geeft de wettelijk vertegenwoordiger toestemming om deze informatie te delen met de financierende partij.

<u>Toestemmingsformulier uitwisselen informatie met derden</u>:
In het kader van onder andere de Jeugdwet, is het niet mogelijk gegevens uit te wisselen met andere instanties zonder schriftelijke toestemming van de betrokkene (tenzij dit niet wettelijk verplicht is). In deze gevallen is het nodig een papieren toestemmingsverklaring te ondertekenen, bijvoorbeeld wanneer je contact wil opnemen met de leerkracht of andere hulpverlenende instantie. In dat geval wordt dit formulier voorgelegd. In dezelfde regels is vastgelegd dat alle medewerkers van Stichting ROOZ gehouden zijn aan zorgvuldigheid met betrekking tot het verwerken van persoonsgegevens. Op de uitwisseling is de Algemene Verordening Gegevensbescherming van toepassing. Er wordt alleen informatie gevraagd en verstrekt die noodzakelijk is voor een adequate hulp aan de cliënt. Andere mogelijke informatie die niet direct dit doel dient, wordt niet verstrekt dan wel gevraagd. Indien informatie wordt uitgewisseld, beschrijft de hulpverlener op het toestemmingsformulier wanneer, met wie (naam en functie), de reden en met welk doel de informatie wordt opgevraagd dan wel verstrekt.

Dit formulier is 1 jaar geldig na datum van tekening. Dit om te voorkomen dat er informatie wordt verstrekt aan personen die niet meer betrokken zijn bij de cliënt.

6.2 Personeelsgegevens

Het aanleggen van een personeelsdossier is toegestaan als dat noodzakelijk is voor het uitvoeren van een arbeidsovereenkomst. Niet alle gegevens mogen in een personeelsdossier voorkomen. Gegevens als klachten, waarschuwingen, verzuimfrequenties, beoordelingsgesprekken en persoonlijke werkaantekeningen van de raad van bestuur worden opgenomen. Ten aanzien van medische gegevens mogen alleen gegevens voor re-integratie en verzuimbegeleiding worden bewaard, zoals informatie over de functionele beperkingen en de noodzakelijke aanpassingen op de werkvloer.

Personeelsdossiers worden 2 jaar na beëindiging van het dienstverband bewaard. In geval van een arbeidsconflict kunnen de gegevens langer worden bewaard.

Gegevens uit de salarisadministratie die fiscaal van belang zijn, worden 7 jaar na beëindiging van het dienstverband bewaard, loonbelastingverklaringen en een kopie van het identiteitsbewijs 5 jaar na beëindiging van het dienstverband.

Gegevens van sollicitanten worden uiterlijk vier weken na afloop van de sollicitatieprocedure bewaard, tenzij de sollicitant toestemming heeft gegeven om de gegevens gedurende een bepaalde tijd in portefeuille te houden.

Toestemmingsverklaring P&O gegevensuitwisseling met derden:
Met dit formulier geeft de medewerker toestemming om gegevens over hem/haar te verwerken. Conform de Algemene verordening gegevensbescherming (AVG) informeert Ko & Zo BV de medewerker over de gegevens die over de medewerker worden uitgewisseld en de gegevens die over de medewerker worden geregistreerd. Dat betekent bijvoorbeeld dat Ko & Zo BV de medewerker uitlegt om welke specifieke gegevens het gaat en waarom deze gegevens noodzakelijk zijn om te delen met derden.

7. Rechten betrokkene

Een belangrijke voorwaarde voor het verwerken van Persoonsgegevens is dat de verwerking rechtmatig, behoorlijk en transparant is. Om daar voor te zorgen moeten de betrokkenen (in het geval van Stichting ROOZ met name onze cliënten en werknemers) op een heldere en volledige wijze worden geïnformeerd over het verwerken van hun persoonsgegevens. Dit betekent ook dat zij goede en volledige informatie krijgen over hun rechten en hoe zij die kunnen uitoefenen. Het informeren van de betrokkenen is behandeld in hoofdstuk 4. In dit hoofdstuk gaat het over de rechten die een betrokkene heeft op grond van de AVG en hoe hij/zij daarvan gebruik kan maken.

7.1 Recht op inzage

De cliënt heeft het recht zich tot de verantwoordelijke te wenden met het verzoek hem mee te delen of zijn persoonsgegevens worden verwerkt. De verantwoordelijke dient de betrokkene schriftelijk binnen vier weken na een daartoe strekkend verzoek mee te delen of dergelijke persoonsgegevens worden verwerkt.

Indien persoonsgegevens van de cliënt worden verwerkt dan bevat de mededeling een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van het doel van de gegevensverwerking, de ontvangers evenals de beschikbare informatie over de herkomst van de gegevens.

Indien een verwerking plaatsvindt door een instantie of dienst voor wetenschappelijk onderzoek of statistiek, en de nodige voorzieningen zijn getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische en wetenschappelijke doeleinden kunnen worden gebruikt, kan de zorgcoördinator weigeren aan een verzoek om inzage te voldoen.

Het recht op inzage kan (tijdelijk) worden beperkt voor zover dit noodzakelijk is ter voorkoming van strafbare feiten, indien in het belang van de bescherming van de cliënt of indien in het belang van de rechten en vrijheden van anderen. Het besluit om het recht op inzage beperken, dient te worden getoetst met het 'juridisch Zwitsers zakmes'. De argumenten op basis waarvan het recht op informatie wordt beperkt, worden zorgvuldig gemotiveerd en gedocumenteerd.

7.2 Recht op correctie of rectificatie

De cliënt kan de verantwoordelijke verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen.

De verantwoordelijke bericht de betrokkene binnen vier weken na ontvangst van het verzoek schriftelijk of dan wel in hoeverre hij daaraan voldoet. Een weigering is met reden omkleed.

De verantwoordelijke draagt ervoor zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd. De verantwoordelijke die persoonsgegevens naar aanleiding van een verzoek heeft verbeterd, aangevuld, verwijderd of afgeschermd, is verplicht om aan derden aan wie de gegevens eerder zijn verstrekt, zo spoedig mogelijk kennis te geven van deze aanpassing, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost.

7.3 Recht van verzet

De cliënt kan bij de verantwoordelijke schriftelijk verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met bijzondere persoonlijke omstandigheden, voor zover de persoonsgegevens worden verwerkt op grond van een gerechtvaardigd belang van de verantwoordelijke of een derde aan wie gegevens zijn verstrekt of de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door een bestuursorgaan. De verantwoordelijke dient binnen vier weken na ontvangst van het verzet te beoordelen of het verzet gerechtvaardigd is. Indien het verzet gerechtvaardigd is beëindigt de verantwoordelijke per direct de verwerking

8. Bijzondere persoonsgegevens, strafrechtelijke gegevens en BSN

Art. 9 lid 1 AVG: Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

De aard van sommige gegevens brengt mee dat de verwerking ervan een grotere inbreuk kan maken op de persoonlijke levenssfeer van de betrokkene omdat die gegevens gevoelige informatie over iemand verschaffen. In de AVG worden deze gegevens 'bijzondere persoonsgegevens' genoemd. Voor de verwerking van deze bijzondere gegevens geldt een verbod, tenzij er een wettelijke uitzondering van toepassing is. Die uitzondering kan in de AVG staan of in een wet van de lidstaten.

8.1 Gezondheidsgegevens

Art. 4 lid 15 ''gegevens over gezondheid'': persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.

Stichting ROOZ mag gezondheidsgegevens van de cliënt verwerken volgens de Uitvoeringswet AVG (art. 23 lid 1)

Wij behoren tot:

- Sub a): Hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene, dan wel het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is;

8.2 Geheimhouding

De medewerker is verplicht tot geheimhouding van hetgeen hem uit hoofde van zijn functie en beroep ter kennis is gekomen. Deze verplichting geldt ook na beëindiging van het dienstverband.

Medewerkers die direct contact hebben met cliënten hebben uit de aard van hun werk veel privacygevoelige gegevens nodig. In de meeste gevallen dienen zij ieder moment over die gegevens te kunnen beschikken. Voor hen geldt dat zij bewust moeten zijn van hun bijzondere positie en maatregelen treffen om de privacy van de cliënt te beschermen. Cliëntgegevens worden indien mogelijk digitaal aangeleverd, door middel van het elektronisch cliënt registratie systeem, indien papieren versie genoodzaakt is, standaard vervoerd in een gesloten envelop of map. Cliëntgegevens dienen uitsluitend in overleg met de Raad van Bestuur vervoerd te worden en mogen nooit in de auto achterblijven. Persoonsgegevens worden alleen ter beschikking gesteld aan de bevoegde medewerkers.

8.3 Burgerservicenummer

AVG ziet een nationaal identificatienummer in beginsel als een ''gewoon'' persoonsgegeven. Lidstaten kunnen echter specifieke voorwaarden stellen voor een nationaal identificatienummer of enige andere identificator van algemene aard (art 87 AVG).

Nederland houdt vast aan de lijn die ook onder de Wbp gold. Dat betekent dat voor gebruik van het BSN er een expliciete wettelijke grondslag moet zijn die verwerking toestaat.

art. 44 Uitvoeringswet Avg: Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald.

Stichting ROOZ mag volgens de uitvoeringswet AVG het burgerservicenummer verwerken. Deze is nodig om cliënten te identificeren om zo declaraties te kunnen doen bij de desbetreffende gemeenten / zorgkantoren.

9. Bewaartermijnen (zie de bijlage 3)

De AVG bepaalt dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor het realiseren van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt (art. 5 lid 1 sub e AVG).

De algemene regel is dat een organisatie zelf bepaalt aan de hand van het doel hoe lang de gegevens bewaard moeten worden. Maar de uitzonderingen hierop zijn weergegeven in bepaalde wetgeving, zoals de WGBO en het Burgerlijk Wetboek. In deze paragraaf worden de bewaartermijnen van cliënt en personeelsgegevens weergegeven, deze zijn gebaseerd op onderstaand genoemde wetgeving.

9.1 Bewaren van cliëntgegevens

Persoonsgegevens die betrekking hebben op de uitvoering van de overeenkomst worden vernietigd na beëindiging daarvan. Voor alle duidelijkheid, dat geldt niét voor de dossiers. Daarvoor geldt een wettelijke bewaartermijn. Daartoe is in de Selectielijst 2017 (8.1.2) en in Jeugdwet (artikel 7.3.8 en 7.3.9) bepaald dat de jeugdhulpverlener het dossier bewaart gedurende vijftien jaar, te rekenen vanaf het tijdstip van ontvangst of waarop zij door de jeugdhulpverlener is vervaardigd, of zoveel langer als redelijkerwijs uit de zorg van een goed jeugdhulpverlener voortvloeit

Gegevens die niet medisch van aard zijn, worden niet langer bewaard dan noodzakelijk, tenzij deze gegevens zijn geanonimiseerd.

Stichting ROOZ verwerkt en bewaart gegevens die van medische aard zijn (hieronder valt ook het dossier van de cliënt). Dit betekent dat wij deze gegevens 15 jaar bewaren in het cliëntdossier.

9.2 Bewaren van personeelsgegevens

Het aanleggen van een personeelsdossier is toegestaan als dat noodzakelijk is voor het uitvoeren van een arbeidsovereenkomst. Niet alle gegevens mogen in een personeelsdossier voorkomen. Gegevens als klachten, waarschuwingen, verzuimfrequenties, beoordelingsgesprekken en persoonlijke werkaantekeningen van de raad van bestuur worden opgenomen. Ten aanzien van medische gegevens mogen alleen gegevens voor re-integratie en verzuimbegeleiding worden bewaard, zoals informatie over de functionele beperkingen en de noodzakelijke aanpassingen op de werkvloer.

- Personeelsdossiers worden 2 jaar na beëindiging van het dienstverband bewaard. In geval van een arbeidsconflict kunnen de gegevens langer worden bewaard.
- Gegevens uit de salarisadministratie die fiscaal van belang zijn, worden 7 jaar na beëindiging van het dienstverband bewaard, loonbelastingverklaringen en een kopie van het identiteitsbewijs 5 jaar na beëindiging van het dienstverband.
- Gegevens van sollicitanten worden uiterlijk vier weken na afloop van de sollicitatieprocedure bewaard, tenzij de sollicitant toestemming heeft gegeven om de gegevens gedurende een bepaalde tijd in portefeuille te houden.

9.3 Vernietiging van privacy gevoelige gegevens

Als persoonsgegevens niet meer nodig zijn of de bewaartermijn is verstreken, dan dienen de gegevens verwijderd te worden. Onder privacy gevoelige gegevens worden verstaan alle gegevens die herleidbaar zijn tot een individueel persoon: een cliënt of een medewerker. Documenten met privacy gevoelige gegevens dienen vernietigd te worden (m.b.v. papierversnipperaar).

De volgende cliëntgebonden documenten bevatten privacy gevoelige gegevens:
- Intakeformulier
- Zorgplannen
- Toestemmingsverklaringen
- Zorgdossiers
- Brieven van derden over de cliënt
- Brieven aan de cliënt
- Klachtenbrieven
- Rapportages
- Persoonlijke werkaantekeningen

De volgende personeelsgebonden documenten bevatten privacy gevoelige gegevens:
- Sollicitatiebrieven
- Verslagen van functioneringsgesprekken
- Verslagen van beoordelingen
- Brieven van en aan medewerkers
- Personeelsdossiers
- Verslagen van verzuimgesprekken en re-integratieplannen

10. ICT beleid

Persoonsgegevens moeten goed beveiligd worden door passende technische en/of organisatorische maatregelen zodat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. (art 5 lid 1 sub f AVG).
Stichting ROOZ heeft de beveiliging van haar systemen hoog in het vaandel staan. Binnen de organisatie wordt gewerkt met gevoelige cliënteninformatie waarbij een goede beveiliging van haar systemen niet kan worden uitgesloten. In het kader daarvan heeft de organisatie een aantal procedures/beleid opgesteld op het gebied van systeembeheer en beveiliging. Aan het einde van dit beleidsdocument zijn de taken, verantwoordelijk- en bevoegdheden beschreven.

10.1 Systeembeheer

Het beheer van de ICT software en de toegang daartoe, is de verantwoordelijkheid van de directeur.
De directeur is de contactpersoon voor de externe partijen.
De directeur speelt een actieve rol in relatie tot ICT beheer. Bij ziekte en/of afwezigheid, verzorgt de zorgmanager een vervangende partij.

10.2 Beveiliging server/systeem

De organisatie beschikt over een algemene schijf (Google Drive) welke voor specifieke medewerkers toegankelijk is. Deze schijf hangt in de Cloud. Echter, niet alle mappen op deze schijf zijn toegankelijk voor alle medewerkers. Welke map toegankelijk is voor iedere medewerker, is afhankelijke van zijn of haar functie binnen de organisatie. De directeur is de beheerder bij het toewijzen van mappen m.b.t. betreffende medewerkers.
De medewerkers kunnen hun 'persoonlijke' documenten ook op de Drive plaatsen, in een eigen map. Deze schijf is alleen toegankelijk als er onder de betreffende medewerker wordt ingelogd. Deze schijf is zo ontwikkeld zodat een medewerker zijn of haar 'persoonlijke' documenten kan bewaren, maar ook documenten kan delen met collega's.
De directeur, zorgmanager en ICT-medewerker beschikken ook over alle gebruikersnamen en wachtwoorden.

10.3 Back-up server

Omdat alle documenten in de Cloud hangen, kunnen documenten niet verloren gaan door hardware/software problemen, diefstal, brand etc. Enig risico is dat de gegevens alleen bereikbaar zijn met internetverbinding.

10.4 Nieuwe gebruiker en inloggen Drive

Het aanmaken van een account voor een medewerker wordt uitgevoerd door de ICT medewerker. Iedere medewerker krijgt de standaard rechten gekoppeld aan een gebruiker. Indien een medewerker andere rechten toegewezen dient te krijgen, dan dient de directeur of ICT medewerker persoonlijk deze mappen te delen. Het inloggen geschiedt altijd met een wachtwoord (geheim) welke door de ICT medewerker wordt aangemaakt. Na het aanmaken van een nieuw wachtwoord, dient de medewerker het wachtwoord via de mail door te geven aan de ICT medewerker. De ICT medewerker bewaart de wachtwoorden en gaat hier zorgvuldig mee om. Indien noodzakelijk kan de directeur of ICT medewerker het wachtwoord van een medewerker gebruiken om onder diens account in te kunnen loggen. Dit gebeurt alleen bij hoge uitzondering, zoals bijvoorbeeld bij ziekte of bij vermoeden van onrechtmatigheden en/of misbruik.
Het afsluiten van een account wordt uitgevoerd door de directeur.

10.5 Webmail

Alle medewerkers van de organisatie die een 'stichtingrooz' e-mailadres hebben toegewezen, kunnen gebruik maken van de webmail via Gmail. De webmail kan ook worden ingesteld op een mobiel toestel. Op deze manier zijn de medewerkers niet gebonden aan het kantoor en flexibeler inzetbaar voor de doelgroep. Voor het inloggen via de webmail kan dezelfde gebruikersnaam en wachtwoord gebruikt worden als op het kantoor.

Risico: Het inloggen via de webmail vereist geen extra beveiliging middels een token, het betreft hierbij geen login op de server van de organisatie en bevat minder gevoelige/beveiligde informatie. De beveiliging via de gebruikersnaam en wachtwoord vindt de organisatie voldoende.

10.6 Wachtwoorden en inlogcodes

Alle wachtwoorden en inlogcodes worden in een document op de Google Drive bewaard. Hiertoe heeft alleen de ICT medewerker en de directeur toegang.

10.7 Virusscanner

De laptops van de organisatie zijn voorzien van een actuele virusscanner. De verantwoordelijkheid voor het beheer en het actualiseren (verlenging licentie) hiervan, ligt bij de directeur.

10.8 Zorgadministratiesysteem ONS
Sinds januari 2019 wordt vanuit Stichting ROOZ gewerkt met het zorgadministratiesysteem ONS, van Nedap Healthcare (Website Nedap). In dit systeem wordt de volledige zorgadministratie van de cliënten van Stichting ROOZ bijgehouden. In deze paragraaf wordt toegelicht hoe de beveiliging door Nedap Healthcare binnen dit systeem en hun applicaties gewaarborgd is.

Beveiliging Nedap Ons
Nedap host alle oplossingen op eigen servers in meerdere beveiligde datacenters in Nederland. De fysieke toegang tot servers en toegangsbeveiliging is dienstverlening die wordt afgenomen van de leverancier van de datacenters waar Nedap healthcare gebruik van maakt. De aanwezigheid van een certificering voor ISO 27001 en een SOC1/SOC2/ISAE3402 verklaring voor Data Center Hosting Services (of vergelijkbaar) is een vereiste voor datacenter(s). Niemand anders dan Nedap - of door Nedap ingeschakelde derden - hebben fysieke toegang tot de servers waarop de zorgsystemen worden gehost. De server zijn eigendom van Nedap.

Logische toegang tot servers wordt enkel verstrekt met op naam gekoppelde accounts. Elke medewerker die logische toegang nodig heeft tot servers, krijgt een eigen account op zijn of haar naam. Voor logische toegang tot servers is altijd two-factor authenticatie nodig: het is niet mogelijk om enkel met een gebruikersnaam en wachtwoord in te loggen op servers. Logging wordt verzameld en afwijkingen worden automatisch gedetecteerd.

De meerdere datacenters zijn replicaties van elkaar, wat betekent dat alle data (nagenoeg) onmiddellijk op alle locaties beschikbaar is. Dit betekent dat bij een storing of incident in één van de datacenters de klantdata nog steeds beschikbaar is.

Alle klantomgevingen zijn logisch van elkaar gescheiden; zo heeft elke omgeving een eigen database. Minimaal 4 keer per dag wordt van elk van deze databases een logische backup gemaakt. Dit is een backup waarin enkel gegevens van die ene klantomgeving staan. Elke back-up die gemaakt wordt, wordt eerst lokaal in het datacenter opgeslagen waar de data op dat moment beschikbaar is.

Vervolgens wordt elke backup gekopieerd naar een offsite locatie. Meerdere keren per (werk)dag wordt geautomatiseerd getest of een backup kan worden teruggezet.

Zodra gegevens (back-ups of andere gegevens) onze datacenters verlaten, wordt encryptie toegepast om te voorkomen dat onbevoegden toegang kunnen krijgen tot de gegevens. Voor transport van gegevens via de webapplicaties (zie verderop onder “toegang”) is dat bijvoorbeeld HTTPS met TLSv1.x, geconfigureerd volgens nationale en internationale richtlijnen. Beveiligingsupdates worden binnen 24 uur na beschikbaar stellen, geïnstalleerd op alle servers. Hierop wordt automatisch gemonitord.

Personeel, organisatie & toetsing
Informatiebeveiliging hebben de voortdurende aandacht van onze organisatie. Nedap healthcare heeft personeel in dienst met relevante security-ervaring en -certificeringen (waaronder CISSP). Regelmatig wordt het onderwerp informatiebeveiliging binnen de gehele groep besproken en worden verbeteringen doorgevoerd. Waar nodig wordt externe (specialistische) kennis ingehuurd. Daarnaast worden regelmatig door zowel interne medewerkers als externen testen uitgevoerd op verschillende onderdelen van onze dienstverlening, waaronder security-scans, pentesten en netwerktesten. Ook compliancy-testen op het gebied van bijvoorbeeld servers en configuraties van SSL worden met regelmaat uitgevoerd. General IT-controls en de daarbij behorende security-maatregelen zoals nodig voor IT-auditors (bijvoorbeeld in het kader van een jaarrekeningcontrole) worden getoetst door externe IT-auditors en/of accounts (in 2017: EY).

In overleg staan we altijd open voor aanvullende onderzoeken door klanten. Zo worden er regelmatig door security-bedrijven in opdracht van onze klanten onderzoeken uitgevoerd. Onder bepaalde voorwaarden werken we hier altijd aan mee, om het vertrouwen in (de beveiliging van) onze oplossingen te ondersteunen en onderstrepen.

Koppelvlakken (toegang)
Er zijn grofweg drie manieren om toegang te krijgen tot gegevens in Ons:

- Webtoegang: hierbij gebruikt de gebruiker een webbrowser om in te loggen in de verschillende applicatie(s) om in deze browser gegevens te raadplegen of wijzigen. Hier valt ook het gebruik van een browser op een mobiel device (zoals tablet of smartphone) onder.
- Mobiele apps: hierbij maakt de gebruiker gebruik van een iOS of Android applicatie om (een deel van) de gegevens die beschikbaar zijn in Ons te raadplegen of wijzigen.
- Technische toegang (ook wel Machine-2-Machine communicatie) zoals OnsDB, koppelingen met derden, etc.: dit is toegang door een andere applicatie, zoals bijvoorbeeld BI-tooling, koppelingen met derden of andere vormen van integraties met systemen. Deze technische toegang is een directe koppeling of kopie van de gegevens zoals Nedap die opslaat. Autorisatiemodellen zoals van toepassing bij de Webtoegang en/of Mobiele applicaties zijn hier niet of in verminderde mate van toepassing. De toegang tot gegevens die via een technische koppeling zijn verkregen vallen niet onder de verantwoordelijkheid van Nedap en is verder ook niet beschreven in dit document. Als er gebruik gemaakt wordt van dit soort koppelingen zal met de desbetreffende leverancier afspraken moeten worden gemaakt.

Webapplicaties

Transportbeveiliging

Toegang tot webapplicaties is alleen mogelijk via een beveiligde HTTPS verbinding. Voor de configuratie van deze verbinding hanteren we nationale en internationale richtlijnen, waaronder de "ICTbeveiligingsrichtlijnen voor Transport Layer Security (TLS)" van het Nationaal Cyber Security Centrum (NCSC) en de strenge PCI-DSS richtlijn. Dit houdt (op dit moment) concreet in dat alleen TLSv1.0 of hoger wordt ondersteund met ciphers die Forward Secrecy ondersteunen. Elke maand wordt de bestaande configuratie geëvalueerd en zonodig aangepast. Ook hier geldt dat beveiligingsupdates gerelateerd aan SSL binnen 24 uur na beschikbaar stellen worden uitgerold, veelal zelfs sneller.

Persoonlijke accounts

Voor alle oplossingen van Ons is voor elke gebruiker een persoonlijk inlogaccount nodig. Het delen van accounts -meerdere gebruikers werken met hetzelfde account- wordt door Nedap ten zeerste afgeraden en is in een aantal contexten in de zorg zelfs niet toegestaan. Doordat gebruikers met een persoonlijk account inloggen zijn acties in applicaties (met behulp van auditing en logging) te herleiden naar een persoon. → De inrichting van accounts en de bijbehorende autorisaties is de verantwoordelijkheid van de zorginstelling.

Two factor authenticatie en Firewalling

Een goed wachtwoord biedt een basisniveau van beveiliging. Een zogenaamde "tweede factor" (2FA) is tegenwoordig een passende maatregel die minimaal verwacht mag worden om een adequaat beveiligingsniveau te bereiken in relatie tot de gevoeligheid van de gegevens waarmee wordt gewerkt (vergelijkbare maatregelen worden getroffen bij toegang tot DigID, Online bankieren, e.d.) Ons biedt verschillende vormen van 2FA aan: via SMS, een vaste telefoon en een toegangscode app. Het is mogelijk om 2FA uit te schakelen voor een beperkt aantal IP adressen (vaak gerelateerd aan fysieke locaties). → De zorginstelling bepaalt zelf op welke locatie(s) 2FA uitgeschakeld is. → Ook bepaalt de zorginstelling zelf hoe lang een 2FA sessie in Ons geldig is, afhankelijk van het eigen informatiebeveiligingsbeleid.

Toegang via Mobiele applicaties

De mobiele applicaties van Ons zijn gratis en onbeperkt te downloaden uit de Appstore en Google Play Store. Voordat met de applicaties toegang verkregen kan worden tot gegevens in Ons, moet het device eerst gekoppeld worden aan een gebruiker in Ons. Dit moet de gebruiker zelf doen. Na deze eenmalige koppeling is er met het betreffende device alleen toegang mogelijk tot gegevens waar de gemachtigde gebruiker ook toegang toe heeft. De mobiele applicaties zijn alleen te gebruiken na het invoeren van een PIN code. In het geval van diefstal of verlies van het device is het mogelijk om op afstand het device weer te ontkoppelen.

Uitloggen (time-outs)

Gebruikers die niet meer actief zijn in de webapplicatie worden na verloop van tijd automatisch uitgelogd. Hierna moet je als gebruiker opnieuw inloggen, ook met eventuele 2FA. De tijdsperiode (time-out) van inactiviteit waarna je automatisch wordt uitgelogd is door de zorginstelling zelf te

bepalen, maar Nedap adviseert om hiervoor een zo kort mogelijke periode te kiezen. In de mobiele applicaties wordt de gebruikers na 15 minuten van inactiviteit opnieuw om een PIN code gevraagd.

Mobiele toepassingen
Eigen apparaten (BYOD) Nedap maakt geen verschil tussen privé- of bedrijfstoestellen. Ons uitgangspunt is dat veiligheid altijd geborgd is in de applicaties zelf; onafhankelijk van andere beveiliging op het toestel. Zo is het bijvoorbeeld mogelijk om de koppeling met een toestel te verbreken zonder dat daarvoor het toestel zelf nodig is. Dit is nodig in het geval van verlies of diefstal, en kan door de gebruiker zelf worden gedaan in een webportaal.

Lokale data
Ons applicaties op mobiele telefoons halen via beveiligde verbindingen de gegevens uit Ons die noodzakelijk zijn voor de betreffende applicatie. Gegevens die worden opgeslagen op een mobiele telefoon worden versleuteld opgeslagen en zijn niet toegankelijk voor applicaties anders dan die van Ons. Gegevens die niet (meer) nodig zijn, worden verwijderd.

Technische toegang (Machine-2-Machine)
Voor diverse vormen van integraties en koppelingen die gegevens in Ons betreffen, zijn allerlei koppelingen mogelijk. De aard van deze koppeling verschilt, maar de technische beveiliging is voor alle koppelingen hetzelfde. Voor de technische beveiliging een Machine-2-Machine koppeling (bijvoorbeeld met behulp van API's) wordt gebruik gemaakt van clientcertificaten (two-way SSL certificaten). Een geldig, door Nedap uitgegeven clientcertificaat is vereist voor toegang tot een API. Nedap healthcare beschikt over een eigen Certificate Authority waarmee certificaten kunnen worden uitgegeven aan klanten. Deze certificaten zijn een beperkte tijd geldig en kunnen alleen worden aangevraagd en uitgegeven via Ons Supportportaal. Er wordt gevalideerd of de aanvraag voor een clientcertificaat door de klant wordt gedaan en indien goedgekeurd is een certificaat alleen geldig voor één klant en één koppeling. Het is dus altijd de klant die bepaalt welke derde(n) toegang hebben tot welke gegevens via een koppeling. Ook kan de klant op elk moment de toegang weer intrekken door een certificaat ongeldig te (laten) verklaren of in te trekken.
Voordat een derde partij volledige toegang krijgt tot onze API's wordt een proces doorlopen waarbij de (potentiële) koppeling wordt getoetst op functioneren en wordt getoetst of de technische beveiliging van de koppeling voldoet aan onze eisen.
→ Zodra gegevens door een koppeling vanuit Ons zijn verstrekt aan een derde partij, heeft Nedap geen controle meer over de beveiliging van die gegevens. Daarover moet de klant zelf afspraken maken met de derde partij.

10.9 Website

Op de website van Stichting ROOZ is het aanbod overzichtelijk en gemakkelijk te vinden. Tevens is er veel informatie (over o.m. het kwaliteitsbeleid) te vinden. Op de nieuwspagina houdt de organisatie actief bij welke ontwikkelingen er zijn.

Stichting ROOZ brengt eens per kwartaal een nieuwsbrief uit. Het werven van nieuwe personeelsleden geschiedt eveneens via de eigen website van de organisatie. De eenvoud en de laagdrempeligheid is voor de organisatie een belangrijk uitgangspunt geweest voor het ontwerp. Het actualiseren van de gegevens op de website ligt bij de directeur. De informatie die vermeldt kan worden op de website, kan vanuit verschillende medewerkers van de organisatie worden aangeleverd. Dit zal worden voorgelegd aan de directeur die het uiteindelijk fiat geeft of niet. De CMS van de website is beveiligd middels een gebruikersnaam en wachtwoord.

Webhosting
De webhosting is uitbesteed aan een externe partij (IPPO*). De directeur en ICT medewerker onderhouden de contacten met deze externe partij.

10.10 Telefonie

Stichting Rooz beschikt over 2 mobiele telefoons, per locatie 1. Wanneer de mobiele telefoon na 3 keer overgaan niet wordt opgenomen wordt deze automatisch doorgeschakeld naar de vaste telefoon. Stichting ROOZ beschikt over een vaste telefoon. Nadat de telefoon 5 keer is overgegaan volgt de voicemail op de vaste telefoon en wordt er doorverwezen naar een mobiel nummer voor noodgevallen.
Tevens beschikken de zorgmanager en persoonlijk begeleiders over een mobiele telefoon. Zij hebben allen een voicemail ingesteld.

10.11 Financiële administratie

Exact online : Zie Google Drive\Kwaliteitshandboek\Ondersteunende processen\Financiële administratie
* IPPO: Van Oldenbarneveldtstraat 90 6827 AN Arnhem T: 026 4427870 E: info@ippo.nl

10.12 Privacy waarborging Verwijsindex MULTIsignaal

Bij het afgeven van een signaal in de Verwijsindex, worden persoonsgegevens in de Verwijsindex verwerkt. Volgens de Algemene Verordening Gegevensbescherming (AVG) is er, naast diverse andere redenen, sprake van rechtmatig verwerking van persoonsgegevens, indien dit plaatsvindt in het kader van een wettelijke taak. De Verwijsindex is specifiek benoemd in de Jeugdwet (§7.1). De verwerking van persoonsgegevens is gekoppeld aan deze wettelijke taak (doelbinding), waardoor wij niet meer gegevens bewaren dan noodzakelijk. De regionale Verwijsindex van MULTIsignaal is op deze manier opgezet: gekoppeld aan de doelbinding van de landelijke Verwijsindex én de bijbehorende wettelijke taak van het college van B&W zoals verwoord in de Jeugdwet.

10.13 Medische informatica - Informatiebeveiliging in de zorg

Wij verwijzen over medische informatica en informatiebeveiliging in de zorg naar een document genaamd NEN 7510 WBP, te vinden in het kwaliteitshandboek-ondersteunende processen-kwaliteitsmanagement-Wet bescherming persoonsgegevens

10.4 Mail verkeer

Stichting ROOZ deelt alleen inhoudelijke informatie via ONS.

Mailverkeer met daarin persoonlijke cliëntgegevens zullen beperkt worden door enkel initialen te noemen en evt. de laatste 3 cijfers van het BSN zonder extra gegevens. Zodra er bijzondere persoonsinformatie wordt gedeeld zal dit via een beveiligd mailsysteem worden verzonden. Het versturen van verkoopfacturen gebeurt niet meer via Gmail maar via WeTransfer. Met het WeTransfer Plus abonnement is er de mogelijkheid om een wachtwoord aan het bericht te koppelen waarmee de inhoud van het bericht is gewaarborgd. Via Gmail zal apart een mail worden verzonden met daarin het wachtwoord voor het WeTransfer bericht. Arbeidscontracten en formulieren met persoonlijke gegevens zullen niet meer per mail maar per post worden verzonden, of persoonlijk afgeven.

11. Datalekken

Een datalek is een ''inbreuk in verband met persoonsgegevens''. Dat is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (art. 4 lid 12 AVG).

Datalek binnen 72u melden: Een datalek moet door de verantwoordelijke zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72u na kennisname aan de toezichthoudende autoriteit worden gemeld. In Nederland is dat de Autoriteit Persoonsgegevens. Daarbij moet ten minste het volgende omschreven / meegedeeld worden (art 33 lid 1 en 3 AVG):

a) de aard van de inbreuk, waar mogelijk o.v.v. categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

b) de naam en contactgegevens van de FG of een ander contactpunt;

c) waarschijnlijke gevolgen van de inbreuk;

d) de maatregelen die de verantwoordelijke heeft voorgesteld of genomen om de inbreuk aan te pakken, waaronder in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen

Wanneer het niet mogelijk is alle informatie gelijktijdig te verstrekking kan dat in fases.
(Voorlopig) Melden is dan belangrijker dan volledig zijn (art 33 lid 4 AVG).

Zie ook kwaliteitshandboek “stappenplan datalek”

12. Privacy Impact Assessment (PIA)

Met een PIA (in de AVG een ‘gegevensbeschermingseffectbeoordeling’ genoemd en in de Engelse versie een DPIA) kan aangetoond worden dat bij hoog risico verwerkingen aan de wet voldaan wordt.

Een PIA is een proces gemaakt om een verwerking te omschrijven, de noodzakelijkheid en proportionaliteit van een verwerking te onderzoeken en de risico's en rechten en vrijheden van betrokkenen te managen (door deze te onderzoeken en passende maatregelen te bepalen).

13. Verwerker

Een verwerker (onder de Wbp de ''bewerker'') is in de AVG als volgt gedefinieerd: "Verwerker": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;".

13.1 Verwerkersovereenkomst

Het is verplicht met een verwerker een overeenkomst te sluiten. Stichting ROOZ mag alleen zaken doen met betrouwbare verwerkers die voldoende garanties bieden (art 28 lid 1 AVG). Om die reden dient er een overeenkomst gesloten te worden met de verwerker die bindende aanspraken geeft aan Stichting ROOZ en vergewissen wij ons ervan dat de beveiliging van de verwerker op orde is.

De verwerkers waarmee Stichting ROOZ een verwerkingsovereenkomst heeft, staan in het verwerkingsregister. Zie; google drive -> kwaliteitsmanagement -> AVG

Bijlage 1

Procedure Verwerkingsregister

Titel document Privacy beleid Stichting ROOZ		**Nummer** 2.1
Evaluatiedatum / procedure Februari 2021	**Status** Vastgesteld door de kwaliteitscommissie	**Datum uitgifte** Maart 2019

Vanaf 25 mei 2018 hoeven organisaties de gegevensverwerkingen niet meer te melden bij de Autoriteit, maar hebben zij conform artikel 30 AVG een documentatieplicht. Dit houdt in dat een organisatie met documenten moet kunnen aantonen dat zij de juiste organisatorische en technische maatregelen heeft genomen om aan de wet te voldoen (accountability).

Per verwerkingsactiviteit zal de verantwoordelijke het volgende moeten registreren:

- de naam en contactgegevens van de verantwoordelijke, eventuele gezamenlijke verwerkingsverantwoordelijken en de Functionaris Gegevensbescherming (de FG);
- de doeleinden voor gegevensverwerking;
- een beschrijving van de categorieën betrokkenen en categorieën persoonsgegevens;
- de (voorgenomen) categorieën ontvangers;
- een vermelding van een verstrekking van persoonsgegevens aan een derde land of een internationale organisatie;
- de (voorgenomen) bewaartermijnen en
- een algemene beschrijving van de beveiligingsmaatregelen.

Verder dient het register schriftelijk opgesteld te zijn, waaronder in een elektronisch format. Naast het opstellen, moet het register ook bijgehouden worden. Vervolgens dient er met behulp van de IT-afdeling het register opgezet te worden en bijgehouden. Aangezien deze periodiek geüpdatet dient te worden, is extra ondersteuning nodig. Ook hulpmiddelen kunnen hierbij helpen, zoals automatische meldingen op het moment dat nieuwe soorten gegevens worden verwerkt.

Binnen Stichting ROOZ is een functionaris gegevensbescherming (FG) aangewezen. De FG is verantwoordelijk voor het up to date houden van het verwerkingsregister.

Werkwijze
In beginsel zal er een inventarisatieproces plaatsvinden waarbij alle gegevensverwerkingen- en stromen in kaart worden gebracht. Dit is de basis voor het register en zal meer inzicht geven in de soorten gegevensverwerking.

Per kwartaal zal er een moment ingepland worden om het register te controleren op juistheid en volledigheid. FG is verantwoordelijk voor het aanpassen van gegevensstromen, procedures en zal hierbij om input van collega's vragen omtrent zorginhoudelijke werkzaamheden en IT werkzaamheden.

Bijlage 2

Functie omschrijving Functionaris gegevensbescherming

Verplichte FG

Stichting Rooz is verplicht een FG aan te stellen. Een FG is wettelijk verplicht in drie situaties:

- ➢ Bij overheidsinstanties en publieke organisaties;
- ➢ Voor organisaties die vanuit hun kernactiviteiten (*de processen die essentieel zijn om de doelen van de organisatie te bereiken of die tot de hoofdtaken van de organisatie horen*) op grote schaal individuen volgen. Het kan hierbij gaan om bijvoorbeeld profilering van mensen voor het maken van risico-inschattingen. Relevant hierbij zijn onder meer het aantal betrokkenen en aantal gegevens en de tijdsduur van het volgen.
- ➢ Als op grote schaal bijzondere persoonsgegevens verwerkt worden als kernactiviteit. Bijvoorbeeld gezondheidsgegevens, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden.

Bij Stichting Rooz is er sprake van verwerkingen waarbij stelselmatige observatie van cliënten nodig is. Gezien aard, omvang en doelstelling van de verwerking en grootschalige verwerking van bijzondere persoonsgegevens is een FG bij Stichting Rooz verplicht.

Onafhankelijkheid en geen belangenverstrengeling
De FG moet zijn functie in onafhankelijkheid kunnen uitvoeren en geen instructies ontvangen over het uitvoeren van zijn/haar taken. Hij/zij heeft ook ontslagbescherming die gerelateerd is aan de uitvoering van die taken.

FG mag binnen de organisatie niet (ook) een functie hebben waarin hij/zij het doel en middelen van een gegevensverwerking bepaalt. Dit kan bijvoorbeeld zo zijn als de FG een managementpositie vervult als hoofd financiën, strategie, marketing, IT of HR. Een FG mag andere taken vervullen maar het mag niet leiden tot een belangenconflict. De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de organisatie. Dit is een wettelijke eis.

Privacy kennis en bedrijfskennis vereist

- ➢ Van een FG wordt verwacht dat hij of zij bovengemiddelde vakkennis heeft van privacywetgeving en de praktijk van gegevensbescherming. Waaronder:
- ➢ kennis van nationale en Europese privacywet- en regelgeving over gegevensbescherming;
- ➢ begrip van de gegevensverwerkingen die de organisatie uitvoert;
- ➢ begrip van IT en informatiebeveiliging;
- ➢ kennis van de organisatie en de sector waarin die actief is;
- ➢ het kunnen promoten van een cultuur van gegevensbescherming binnen de organisatie

Taken FG

- ➢ Het informeren over verplichtingen die voortvloeien uit de AVG, de Uitvoeringswet AVG en andere regelgeving op het gebied van de bescherming van persoonsgegevens;
- ➢ Toezien op de naleving van de AVG en de aanpalende regelgeving;
- ➢ Toezien op naleving van het Privacybeleid;
- ➢ Toewijzen van verantwoordelijkheden op het gebied van het verwerken van persoonsgegevens;
- ➢ Creëren van awareness bij degenen die betrokken zijn bij het verwerken van persoonsgegevens;
- ➢ Het uitvoeren van specifieke monitoringsacties;
- ➢ Adviseren over en betrokkenheid bij Privacy Impact Analyses;

- ➢ Samenwerken met de Autoriteit Persoonsgegevens en eventuele andere (Europese) toezichthouders;
- ➢ Fungeren als contactpunt voor de Autoriteit Persoonsgegevens. Contacten met de Autoriteit Persoonsgegevens lopen altijd via de FG.
- ➢ Fungeren als contactpunt voor betrokkenen (bijvoorbeeld cliënten en medewerkers van Stichting Rooz) wanneer dat relevant is wanneer zij gebruik willen maken van de rechten die zij op grond van de AVG hebben;
- ➢ Het voorzitten van het operationele privacy-overleg (Privacy Tafel).
- ➢ Het wijzigen van het Privacybeleid na afstemming in de Privacy Tafel. Over niet materiële wijzigingen informeert de FG de CRO van de Raad van Bestuur. Zonder tegenbericht zijn niet materiële wijzigingen na twee weken van kracht.

De contactgegevens van de FG moeten bekend worden gemaakt bij de Autoriteit Persoonsgegevens.

Stichting Rooz moet er voor zorgen dat de FG tijdig betrokken wordt bij zaken die te maken hebben met de bescherming van persoonsgegevens. Ook zorgt Stichting Rooz er voor dat de FG zijn taken naar behoren kan uitoefenen door hem/haar toegang te geven tot persoonsgegevens en verwerkingsactiviteiten en hem/haar de nodige middelen ter beschikking te stellen. Daartoe hoort ook het kunnen volgen van opleidingen en seminars om zijn deskundigheid op peil te houden.

De FG kan (een deel van) zijn/haar taken delegeren aan anderen.

De instelling van een FG dient verder om de medewerkers in hun communicatie met de cliënten te ondersteunen en om cliënten en medewerkers te woord te staan bij vragen, bijvoorbeeld bij het uitoefenen van hun rechten. *Ook hier geldt dat de FG deze taken kan delegeren.*

Binnen Stichting Rooz wordt de FG ondersteunt door de interne projectgroep welke is samengesteld ten behoeve van alle vragen rondom AVG. Deze bestaat uit de volgende personen:

Wendy Ruijsch (zorginhoudelijk)
Patrick van Bavel (IT)
Marco Cattel (directeur)

Bijlage 3 bewaartermijnen	**Waar te vinden?**	**Bewaartermijn**	**Verantwoordelijke**
Clientgegevens	V.a. 1-2019 ONS 2015-2018 ZilliZ, <2015 Brandkast	Medische gegevens: 15 jaar na beëindiging van zorg. Overig: 10 jaar na beëindiging zorg.	Kwaliteitscoördinator
Personeelsgegevens	Digitaal cliëntdossier Oude personeelsgegevens in mappen in brandkast	Salaris gegevens (fiscaal belang): 7 jaar na beëindiging dienstverband. ID-bewijs & loonbelasting verklaring: 5 jaar Overig: 2 jaar na beëindiging dienstverband *wanneer er een arbeidsconflict speelt, worden gegevens langer bewaard.	Administratief medewerker (P&O)
Administratie	Exact online (boekhoudsysteem vanaf 2015) Job (boekhoudsysteem tot 2013) Loon (salarisadministratie Google Drive, ondersteunende processen, financiële administratie (debiteurenadministratie) Brandkast: mappen administratie stichting (crediteurenadministratie) ONS facturatie en zorgadministratie	7 jaar: loonadministratie, jaarrekeningen, facturen, grootboekadministratie, debiteuren en crediteuren administratie, stukken over ontbinding van rechtspersoon.	Financieel medewerker
Registratie brandweer	Dossierkast, bovenste schap	5 jaar	Kwaliteitscoördinator

Registratie legionella	Dossierkast, bovenste schap	5 jaar	Kwaliteitscoördinator
Registratie schoonmaak werkzaamheden	Dossierkast, bovenste schap	5 jaar	Kwaliteitscoördinator
Registratie keuring speelgoed	Dossierkast, bovenste schap	5 jaar	Kwaliteitscoördinator
Meldingsformulieren (MIC, kindermishandeling, agressie)	V.a. 1-2019 ONS (2015-2018 ZilliZ, > 2015 Brandkast)	5 jaar	Kwaliteitscoördinator
Notulen en agenda's overleggen (RvT, MT, ZO, TO)	Google Drive: werkmap, besturingsprocessen, overleggen	RvT & CR & MT: 5 jaar ZO & TO: 2 jaar	Kwaliteitscoördinator
Inwerkprogramma	Google Drive: kwaliteitshandboek, ondersteunende processen, P&O	5 jaar	Kwaliteitscoördinator
Jaarplanning	Google Drive: werkmap, ondersteunende processen	5 jaar	Planner
Declaratieformulieren medewerkers	P&O administratie Google Drive	5 jaar	Administratief medewerker (P&O)
Kwaliteitshandboek	Google Drive: Werkmap Kwaliteitshandboek	10 jaar	Kwaliteitscoördinator
Verbeter- en klachtenformulieren incl. KAV	Google Drive & Dossierkast	5 jaar	Kwaliteitscoördinator
Registraties door de vertrouwenspersoon (geanonimiseerd)	Google Drive & Dossierkast	5 jaar	Vertrouwenspersoon
Auditplanning	Google Drive, werkmap, ondersteunende processen, kwaliteitsmanagement	5 jaar	Kwaliteitscoördinator
Auditrapportage	Google Drive, werkmap, ondersteunende processen, kwaliteitsmanagement	10 jaar	Kwaliteitscoördinator

RIE	Google Drive, werkmap, ondersteunende processen, kwaliteitsmanagement	10 jaar	Kwaliteitscoördinator
Directiebeoordeling	Google Drive, werkmap, besturingsprocessen	Altijd	Directeur
Beleidsplannen	Google Drive, werkmap, besturingsprocessen	Altijd	Directeur