Dataveiligheidsbeleid Interzorg

10-12-2019

Inleiding

Uw privacy is voor Interzorg van groot belang, net als transparantie over de wijze waarop wij gegevens verwerken en beheren. In dit beleid hebben wij de verplichtingen van Interzorg en de rechten van cliënten of hun vertegenwoordigers, medewerkers, vrijwilligers of andere betrokkenen betreffende gegevensverwerking en -beheer beschreven (hierna te noemen: betrokkenen).

In dit beleid staat beschreven wat er met uw persoonsgegevens gebeurt. Welke persoonsgegevens wij vragen, waar we die voor gebruiken, wie ze gebruikt en aan wie we gegevens mogelijk verstrekken. Uitgangspunt daarbij is dat we alleen persoonsgegevens gebruiken indien dat noodzakelijk is en natuurlijk op een veilige manier.

De Europese wetgeving die ten grondslag ligt aan het verwerken van persoonsgegevens is de Algemene Verordening Gegevensbescherming (AVG).

Dit beleid wordt uiteengezet in vier hoofdstukken: Verwerking van persoonsgegevens, Stappen ter beveiliging, Beheersing & controle en Rechten van betrokkenen.

Wijzigingen in deze privacyverklaring
Het kan voorkomen dat de situatie zich voordoet dat dit beleid moet worden gewijzigd. Het meest actuele beleid zal altijd worden gepubliceerd op www.interzorgthuiszorg.nl.

Hoofdstuk 1:Verwerking van persoonsgegevens

Interzorg verwerkt persoonsgegevens, waarvan het grootste deel bijzondere persoonsgegevens betreft. Met deze persoonsgegevens gaan we uiteraard zeer zorgvuldig om. In het volgende hoofdstuk wordt uiteengezet wat de verwerking van persoonsgegevens inhoudt.

1.1 Definitie persoonsgegevens

Een persoonsgegeven is informatie over een persoon die direct of indirect tot een persoon kan worden herleid, met name aan de hand van een naam, een burgerservicenummer, locatiegegevens, een online gebruikersnaam of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

1.2 Definitie gegevensverwerking

Onder gegevensverwerking wordt verstaan het geheel van bewerkingen met betrekking tot persoonsgegevens 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, combineren, afschermen, wissen of vernietigen van gegevens.

1.3 Doel van het verwerken van persoonsgegevens

Interzorg verwerkt persoonsgegevens met als hoofddoel kwaliteitszorg te kunnen leveren. Het verwerken van deze gegevens gebeurt alleen als dit noodzakelijk is voor:

- de uitvoering van een overeenkomst.
- het nakomen van een wettelijke verplichting.
- bescherming van de vitale belangen.

1.4 Welke gegevens verwerkt Interzorg?

1. Algemene persoonsgegevens (naam, geboortedatum, burgerlijke staat, etc.), contactgegevens (ook van wettelijk vertegenwoordiger), verzekeringsgegevens, verleende zorgproducten, sociaal profiel / netwerk, medische en gedragsgegevens, voor zover relevant voor het naleven van de overeenkomst.
Deze gegevens gebruiken we voor onze bedrijfsvoering, correspondentie en persoonlijke communicatie.

2. Client-/medewerkersnummer
Iedere medewerker en cliënt van Interzorg heeft een uniek registratienummer voor de relatie die we met de betrokkene hebben. Dit nummer is alleen voor Interzorg te herleiden naar de betrokkene.

3. Burgerservicenummer (BSN)
Dit nummer hebben we nodig om gegevens met betrekking tot de betrokkene uit te wisselen met bij voorbeeld het zorgkantoor, een zorgverzekeraar, de belastingdienst of andere zorgaanbieders; gebruik van dit nummer is dan verplicht.

4. Medisch/specialistische, gedragsgerelateerde, sociaal-maatschappelijke en verpleegkundige/begeleidings- gegevens.
Deze gegevens gebruiken we voor het vaststellen, toetsen, volgen en uitvoeren van de individuele zorg- en dienstverlening.

5. Aard van toegepaste vrijheid beperkende middelen of maatregelen voor cliënt, datum, duur, reden, wiens verantwoordelijkheid en de betreffende woning.
Het vastleggen van deze gegevens is nodig om vrijheid beperkende middelen of maatregelen te kunnen toepassen en om te kunnen verantwoorden waarom deze maatregelen noodzakelijk zijn.

6. Toegediende medicatie
Met af te tekenen medicatielijsten maken wij inzichtelijk welke medicatie cliënten hadden moeten ontvangen en of ze deze ook daadwerkelijk hebben ontvangen.

7. Omschrijving en aard van incidenten met betrekking tot cliënten of medewerkers, getroffen maatregelen en schade/letsel.

8. Omschrijving en toedracht van (seksueel) misbruik met betrekking tot een persoon, en de ondernomen actie n.a.v. het misbruik.
Deze gegevens hebben we nodig ten behoeve van de naleving van beleid betreffende het (seksueel) misbruik (afhandeling, nazorg en preventie).

9. Bankrekeningnummer
Betrokkenen maken aan ons kenbaar vanuit welk bankrekeningnummer ze aan financiële verplichtingen willen voldoen.

1.5 Overige persoonsgegevens
Gegevens dienen altijd met een omschreven doel te worden vastgelegd. Bepaalde bijzondere persoonsgegevens (bijvoorbeeld godsdienst, geaardheid, politieke voorkeur en ras) mogen wij niet zomaar vastleggen. In een aantal situaties kan toestemming hiervoor een uitzondering vormen.
Bij voorbeeld pasfoto's, deze kunnen iets over iemands ras zeggen. Wanneer we foto's willen vastleggen voor onze eigen registratie of om ergens te publiceren, kan uw toestemming als basis worden gebruikt om dit toch mogelijk te maken. Toestemming hiervoor kan door de betrokkene op elk moment weer worden ingetrokken.
Euthanasieverklaringen en reanimatieverklaringen worden alleen op verzoek van de cliënt vastgelegd.

Wanneer Interzorg een gerechtvaardigd belang heeft om gegevens te verzamelen en vast te leggen, mag dit zonder toestemming worden gedaan. Denk dan bijvoorbeeld aan agressief gedrag dat voor onze medewerkers van belang is om te weten.

1.6 Hoe verkrijgt Interzorg de persoonsgegevens?
Interzorg kan gegevens rechtstreeks van de betrokkene ontvangen, bijvoorbeeld van een sollicitant of een cliënt.
Daarnaast kunnen gegevens worden ontvangen van derden, met als doel een zorgvuldige overdracht en uitwisseling vorm te geven.

1.7 Hoe verwerkt Interzorg persoonsgegevens?
Persoonsgegevens worden op verschillende manieren verwerkt, dit kan bijvoorbeeld zijn in een digitaal dossier, een papieren dossier, middels een formulier, als papieren notitie, via fax of via (digitaal) berichtenverkeer.

1.8 Van wie verwerken wij persoonsgegevens?
We verwerken persoonsgegevens van onder andere cliënten, medewerkers, sollicitanten, vrijwilligers, (website)bezoekers en externe partijen.

1.9 Termijnen van bewaring
Bij het vaststellen van bewaartermijnen van persoonsgegevens zijn de wettelijke bewaartermijnen leidend.
Per document wordt vastgesteld welke van de vastgelegde persoonsgegevens bewaard moeten blijven om te voldoen aan de wettelijke bewaartermijnen. Zo kan het zijn dat binnen een document een deel van de gegevens verwijderd wordt omdat het conform de wet niet meer noodzakelijk is om deze te bewaren, terwijl een ander deel van het document nog wel bewaard moet blijven.
Interzorg hanteert de volgende bewaartermijnen:

- Personeelsgegevens: 2 jaar na uitdiensttreding, conform de AVG.
- Fiscale gegevens: 7 jaar, conform de Algemene Wet inzage Rijksbelastingen (AWR).
- Sollicitatiegegevens: 4 weken na einde sollicitatieprocedure of na overleg 1 jaar, conform de AVG.
- Medische gegevens (cliëntdossier): 20 jaar na einde behandeling, conform de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO).

1.10 Toestemming

Voor het verwerken van uw persoonsgegevens vragen wij u altijd om toestemming.

- Als cliënt van Interzorg vragen we uw toestemming middels het tekenen van de zorgovereenkomst.
- Als medewerker vragen we uw toestemming middels het tekenen van de arbeidsovereenkomst.
- Overige partijen vragen we toestemming middels een overeenkomst.

1.11 Register van verwerkingen

Omdat Interzorg een organisatie is met meer dan 500 medewerkers die structureel persoonsgegevens en bijzondere persoonsgegevens verwerkt wanneer daar aanleiding toe is, heeft Interzorg een dataverwerkingsregister opgesteld ten behoeve van de meest voorkomende persoonsgegevensverwerkingen.
In dit register staan de volgende elementen beschreven:

- De doelen en de middelen van de verwerking
- Categorieën van betrokkenen
- Categorieën van persoonsgegevens
- Wettelijke bewaartermijnen
- Ontvanger gegevens
- Frequentie van verwerking
- Getroffen beveiligingsmaatregelen

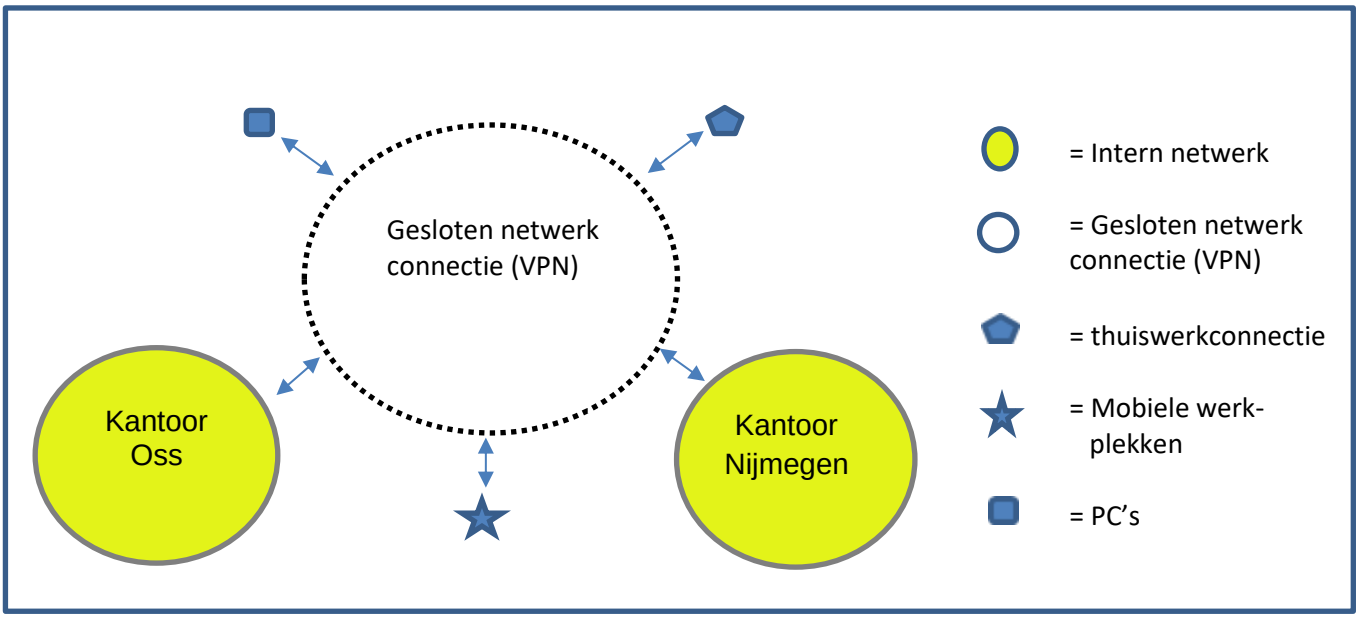
Hoofdstuk 2: Stappen ter beveiliging

Onder informatiebeveiliging wordt verstaan: ‘het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen’.

2.1 Interzorg in beeld

Interzorg werkt vanuit de visie ‘anywhere, anyplace, anytime’ en heeft twee vaste kantoorlocaties ter beschikking. Dit betekent dat er niet alleen vanuit onze kantoorlocaties wordt gewerkt, maar dat medewerkers onafhankelijk van tijd, plaats, of ruimte kunnen werken op de servers van Interzorg.

Interzorg is zich ervan bewust dat 80% van datalekken te wijten is aan de gebruiker en slechts 20% aan systemisch falen (https://www.infosecuritymagazine.nl/wp-content/uploads/2016/10/ISM-4.pdf). Het systeem voldoet aan de hoogste systeembeveiligingseisen conform hedendaagse markt. De getroffen systemische beveiligingseisen kunnen alleen optimaal worden benut als er bewust bekwaam mee om wordt gegaan. Bewustwording is dan ook een terugkerend onderwerp binnen de gehele organisatie.



Figuur 1: Weergave van het systeem en de daarin voorkomende connecties en werkplekken

Interzorg faciliteert haar personeel met PC’s, mobiele telefoons en thuiswerkmogelijkheden (zie ook figuur 1). Er is hierbij altijd sprake van een beveiligde verbinding doordat deze beschermd zijn met zowel een unieke gebruikersnaam en wachtwoord als een zogenaamde two-way authentication factor.

2.2 Connectiviteit

Interzorg biedt kwaliteitszorg, wat bijdraagt dat mensen zolang mogelijk plezierig in hun eigen huis kunnen blijven wonen. Thuiszorg verlenen we bij de mensen thuis en vanuit daar organiseren we voor het grootste gedeelte de zorg. Medewerkers zijn daarom uitgerust met mobiele werkplekken (telefoons, laptops, tablets) waardoor zij altijd en overal toegang hebben tot de benodigde gegevens. We noemen dat anyplace, anywhere anytime.

Op de kantoorpanden van Interzorg bestaat een eigen internetverbinding, deze wordt niet gedeeld met derden. Er is een zakelijke firewall aanwezig die het externe internetverkeer filtert en hiermee ongewenste verbindingen blokkeert.

2.3 Bewust omgaan met gegevens
Interzorg gaat bewust om met het beschikbaar stellen van gegevens. Data is alleen toegankelijk voor gebruikers wanneer dit noodzakelijk is voor het uitvoeren van werkzaamheden.
Gebruikersprofielen maken het mogelijk dat een gebruiker enkel toegang heeft tot data waartoe deze gebruiker is gemachtigd. Dit staat gedocumenteerd in het kwaliteitshandboek.
Bij medewerkers is het creëren van bewustwording geborgd in de inwerkprocedure, tussentijdse scholing, teamoverleggen, informatiebijeenkomsten, individuele gesprekken en publicaties. Door dataveiligheid een repeterend onderwerp te laten zijn wordt bewustwording op peil gehouden dan wel vergroot.
Cliënten worden hierover voorgelicht door wijkverpleegkundigen, voorvrouwen en zorgverleners. Ook is het een terugkerend thema op tussentijdse evaluaties.

2.4 Wachtwoordbeleid
Interzorg heeft een actief wachtwoordbeleid dat zowel systeemtechnisch als beleidstechnisch wordt toegepast. Het is niet toegestaan om wachtwoorden te delen of op welke manier dan ook op te slaan. Het is niet mogelijk om een wachtwoord automatisch te laten onthouden op bijvoorbeeld een laptop, zodat er niet automatisch ingelogd kan worden op het systeem van Interzorg.

2.5 Cliëntportaal
Interzorg stelt haar cliënten in de gelegenheid om gebruik te maken van een onafhankelijk cliëntsysteem, CarenZorgt. Dit is een platform waarin de gebruiker zelf zijn eigen zorgproces kan regisseren. Gebruikers kunnen hiermee toegang verlenen aan hun directe omgeving en andere professionals uitnodigen. De gebruiker kan via CarenZorgt zelf instellen wie welke rechten tot inzage verkrijgen.
Als gebruiker van CarenZorgt heb je een verantwoordelijkheid om zorgvuldig om te gaan met persoonsgegevens. Gebruikers van CarenZorgt worden hier van bewust gemaakt middels een disclaimer.

Cliënten zijn zelf in de gelegenheid om persoonsgegevens te verstrekken en te verwerken in CarenZorgt. Zie hoofdstuk 4: Rechten betrokkenen.

2.6 Data-opslag
Alle data van Interzorg, exclusief de data van de online applicaties, wordt centraal opgeslagen op de servers van Interzorg. Interzorg werkt in een remote desktopomgeving zodat er geen sprake is van lokale opslag. Toegang is beveiligd door middel van een unieke gebruikersnaam en wachtwoord en door two-way authentication.
Er zijn verschillende toegangsbeveiligingen ingezet om het systeem van Interzorg af te schermen voor derden. Zo zijn er IP-filters actief die enkel geautoriseerde bedrijven/personen toegang geven tot het systeem, werkt men intern met beveiligde verbindingen, en is er voor externe toegang tot het systeem een two-way Authenticatie vereist, gefaciliteerd door een externe dienstverlener.

De servers van Interzorg zijn gevestigd in een afgesloten serverruimte met alarmsysteem. Daarbinnen staan zij in afgesloten kasten. Toegang tot deze ruimte wordt bijgehouden in een loginregister en is enkel voorbehouden aan geautoriseerde gebruikers.
De back-up van Interzorg wordt opgeslagen op een apparaat dat in dezelfde beveiligde ruimte staat. De back-up wordt daarnaast versleuteld op dit apparaat opgeslagen. Er wordt geen gebruik gemaakt van USB-disks, en indien er een kopie van de back-up wordt gemaakt zal deze back-up ten alle tijden versleuteld zijn. De encryptiesleutel wordt extern bewaard, gescheiden van de back-updata.
Er wordt ook gebruik gemaakt van een externe (online) back-up die gegevensverlies tegengaat. Van de lokale versleutelde back-up wordt een kopie gemaakt bij datacenters in Nederland. Het is voor de provider niet mogelijk om de back-upbestanden uit te lezen omdat de encryptiesleutel bij de provider niet bekend is.

2.7 Beveiligd e-mail

Er wordt bij Interzorg gebruik gemaakt van een beveiligde mail-oplossing. Deze mail wordt door een externe partij afgehandeld, waarvan eventuele opgeslagen mails enkel binnen de beveiligde omgeving van Interzorg staan opgeslagen. Ook is er een externe spamfilter actief. Deze dienst wordt gefaciliteerd door een externe website-hoster.

2.8 Virusbeveiliging en updates

Op alle systemen van Interzorg, zowel op de servers als op alle (mobiele) werkplekken, is er een virusscanner actief. Deze wordt dagelijks meermaals voorzien van de nieuwste virus en software-updates. Daarnaast worden alle systemen automatisch geüpdatet met de nieuwste (Microsoft) updates.

Hoofdstuk 3: Beheersing & controle

Interzorg houdt zich voortdurend bezig met het verwerken van persoonsgegevens. Betrouwbaarheid en transparantie zijn daarbij kernwaarden. Er ligt aan het verwerken van persoonsgegevens altijd een wettelijke grondslag ten onder. In een register van verwerkingen heeft Interzorg deze grondslagen vastgelegd (zie hoofdstuk 1.11).

- ✓ Als cliënt geeft u in de zorgovereenkomst toestemming om gegevens te mogen opslaan en te verwerken.
- ✓ Als medewerker geeft u in de arbeidsovereenkomst toestemming om gegevens te mogen opslaan en te verwerken.
- ✓ Als (sub)verwerker geef je in de verwerkersovereenkomst toestemming om gegevens te mogen verwerken en hierin staat ook vastgelegd welke gegevens mogen worden verwerkt.

3.1 ISO/HKZ

Interzorg is HKZ gecertificeerd en volgt de richtlijnen van ISO 27001 & NEN 7510.
Daarmee heeft informatiebeveiliging zowel binnen als buiten de zorgsector onze aandacht en streven we naar de hoogste kwaliteit en mate van beveiliging. Jaarlijks hebben we een terugkerende kwaliteitscontrole waarbij databeleid een vast onderdeel is van de controlecyclus.

3.2 Functionaris Gegevensbescherming

Omdat Interzorg als thuiszorgorganisatie op grote schaal persoonsgegevens verwerkt is er voor gekozen om een functionaris gegevensbescherming (FG) aan te stellen.
De FG is een controller die toeziet op een optimale bedrijfsomgeving en actueel beveiligingsbeleid. Hij/zij adviseert het management over te nemen stappen of het aanpakken van risico's die worden geconstateerd.
De primaire taken van de FG hebben niets te maken met de beslissingspositie over veiligheid, aanschaf of operationeel niveau van systemen en/of beveiliging daarvan en zodoende borgt Interzorg de onafhankelijkheid van de positie van de FG om als controller op te treden en advies te verstrekken.

De FG onderneemt de volgende acties, welke zijn opgenomen in de planning- en controlcyclus:

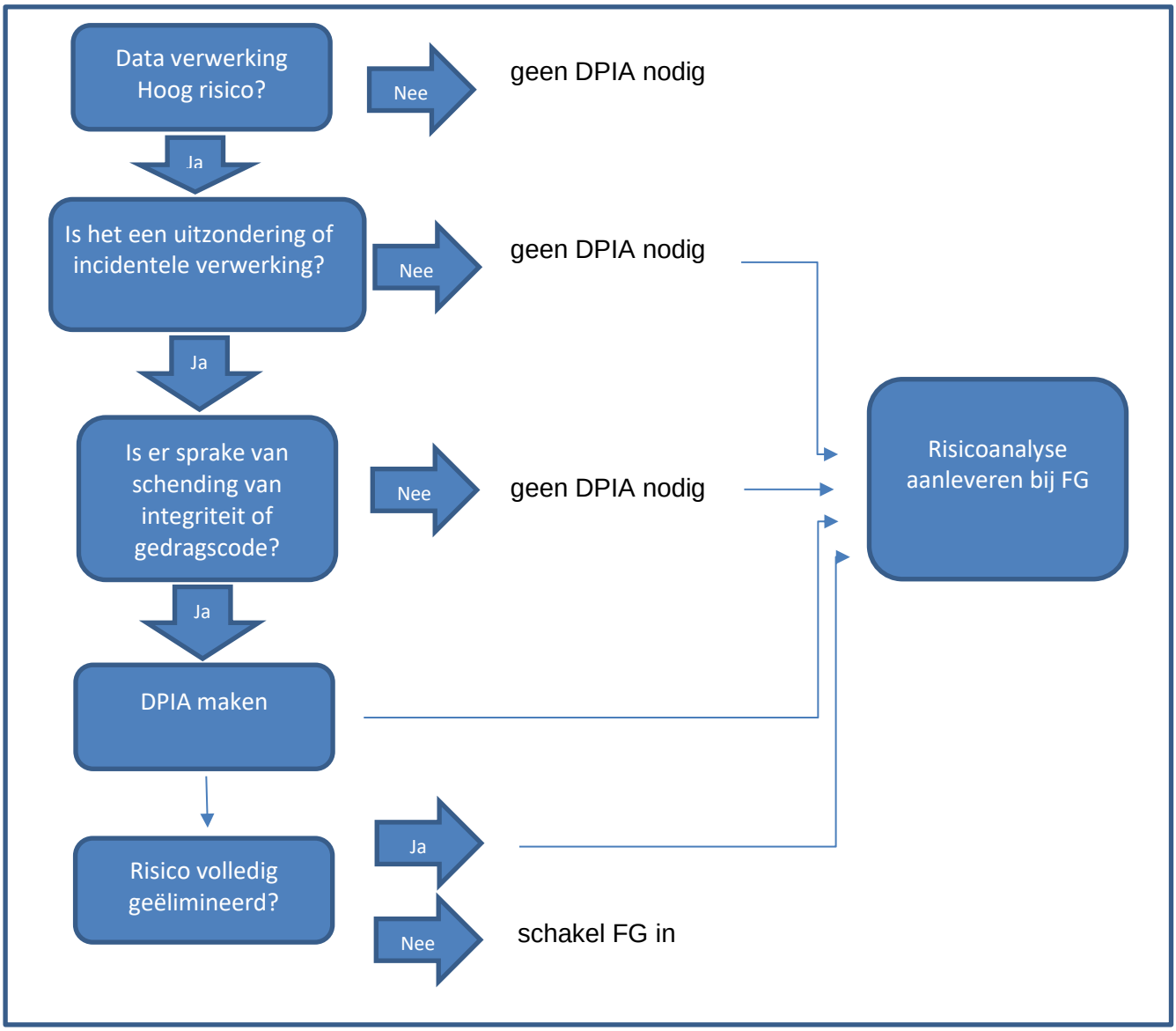
- Informatie verzamelen om verwerkingswerkzaamheden te identificeren
- Analyseren en controleren in hoeverre verwerkingswerkzaamheden aan de AVG voldoen
- De verantwoordelijke of de verwerker informeren, adviseren of aanbevelingen geven

Daarnaast wordt bij (het vermoeden van) een datalek de FG verwittigd.

3.3 Risicosignalering

Interzorg spant zich in om het risico op een datalek (zie hoofdstuk 3.5) tijdig te signaleren en maatregelen te nemen conform een risico-inschatting. Om een goed beeld te krijgen of dataverwerking en informatiebeveiliging mogelijk blootgesteld worden aan mogelijke risico's, zijn de meest voorkomende verwerkingen reeds voorzien van een data privacy impact analyse (DPIA). Het resultaat hiervan is opgenomen in het register van verwerkingen.
Dat geeft aan dat Interzorg haar risico's kent, oplost en daardoor uitsluit en beheerst.

Interzorg gebruikt hiervoor de volgende route:



Figuur 2: Flowchart risicoanalyse. N.B. voor toelichting DPIA zie 3.4.

3.4 DPIA

Wanneer Interzorg een DPIA uitvoert worden de volgende resultaten nagestreefd:

- Een systematische beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan.
- Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen, oftewel: is het verwerken van persoonsgegevens op deze manier noodzakelijk om het doel te bereiken? En is de inbreuk op de privacy van de betrokkenen niet onevenredig in verhouding tot dit doel?
- Een beoordeling van de privacyrisico's voor de betrokkenen.
- De beoogde maatregelen om:
  (1) de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen)
  (2) aan te tonen dat we aan de AVG voldoen.

3.5 Datalek

Bij Interzorg hanteren we de volgende definitie om een datalek te omschrijven:
'Een breuk in de beveiliging wat leidt tot per ongeluk of onwettig verlies, vernietiging, wijzigingen, ongeautoriseerde toegang tot data welke verzonden, opgeslagen of anderzijds verwerkt wordt'.

We kennen drie verschillende types van een datalek:

1. Vertrouwensbreuk: Wanneer er ongeautoriseerd of per ongeluk ontsluiting of toegang tot persoonsgegevens heeft plaats gevonden.
2. Beschikbaarheidsbreuk: Wanneer er ongeautoriseerd of per ongeluk persoonsgegevens verloren raken, vernietigd worden of er geen toegang meer toe is.
3. Integriteitsbreuk: Wanneer er ongeautoriseerd of per ongeluk persoonsgegevens veranderd worden.

Wanneer een medewerker van Interzorg het geringste vermoeden heeft dat er een datalek heeft plaatsgevonden, vult de medewerker direct het daartoe bestemde meldingsformulier ('Formulier melden datalek') in.

Wanneer door Interzorg wordt vastgesteld dat het een datalek betreft, meldt Interzorg het betreffende lek binnen 72 uur bij de autoriteit persoonsgegevens.
Zo ook wanneer er bij een verwerker van persoonsgegevens een lek ontstaat.
Contractueel ligt vast gelegd dat de verwerker verantwoordelijk is om binnen 24 uur het lek bij Interzorg (verwerkersverantwoordelijke) te melden zodat Interzorg het datalek binnen 72 uur kan melden bij de Autoriteit Persoonsgegevens.

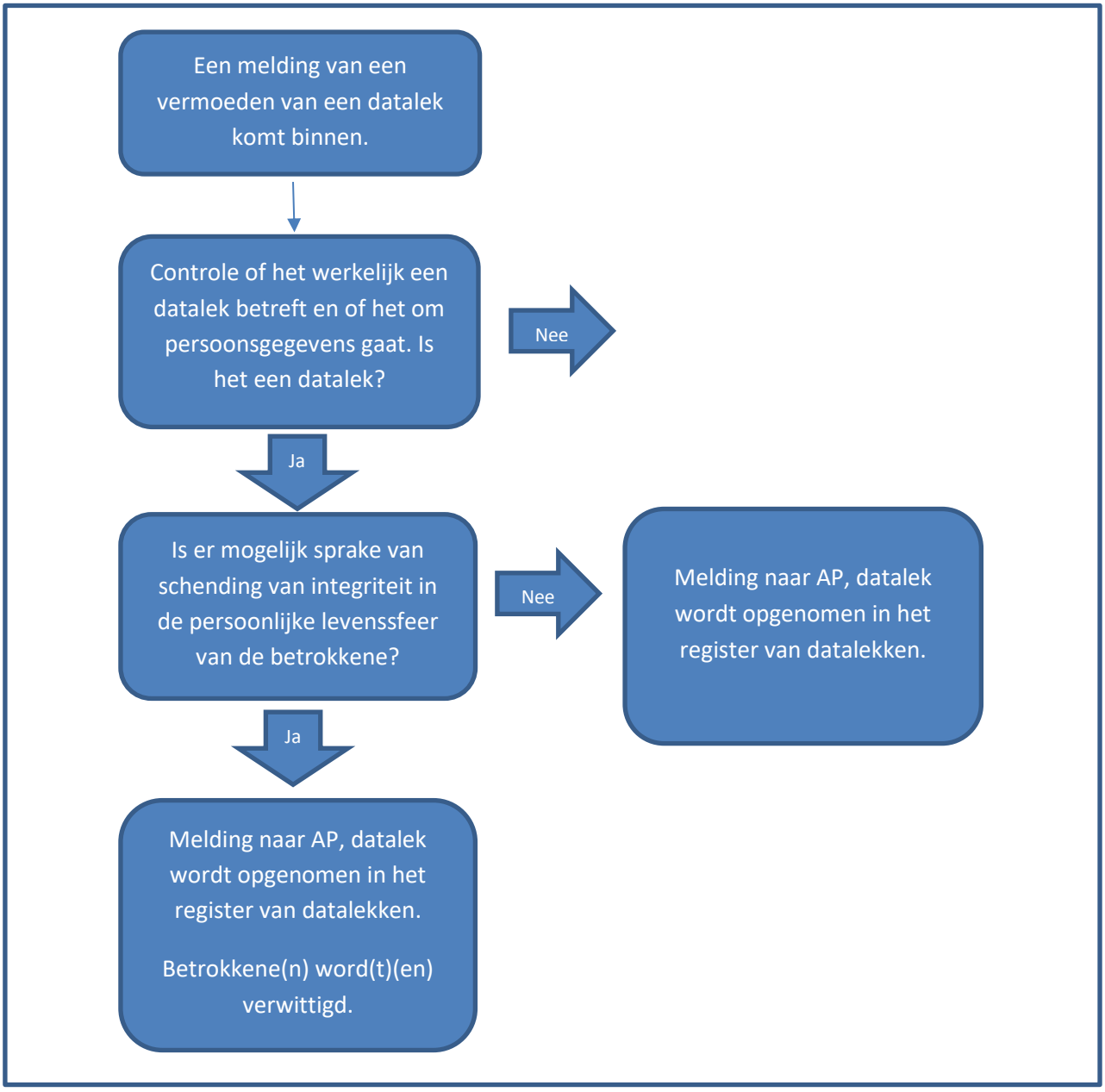
Direct na de melding start een onderzoek waarin gekeken wordt om welke data het gaat, wat het bijbehorende risico is van de verloren data en of en hoe de verloren data mogelijk terug gehaald kunnen worden.

Wanneer er een risico bestaat dat de gelekte gegevens worden gebruikt, misbruikt of mogelijkerwijze in gevaar komen zullen na vaststelling en inschatting van deze risico's de betrokkenen worden verwittigd.
Diegene(n) krijgen tenminste de volgende informatie:

- ✓ Een beschrijving van de aard van het datalek.
- ✓ De naam en wijze waarop de FG benaderd kan worden.
- ✓ Een beschrijving van de mogelijke consequenties het type datalek.
- ✓ Een beschrijving van wat er gedaan wordt, welke maatregelen getroffen worden en hoe de data mogelijk herwonnen wordt.

Wanneer een datalek een grote hoeveelheid data bevat kan er naast persoonlijke gesprekken, e-mails of persoonlijke brieven een melding in de krant gemaakt worden om mensen te informeren dat er sprake is geweest van een groot datalek.

De FG houdt een register bij waarin alle (vermoedens van) datalekken worden bijgehouden.
Tevens monitort de FG of de voorgestelde verbeteringen meetbare resultaten en/of verbeteringen met zich meegebracht hebben binnen het juiste tijdsbestek.



Figuur 3: meldingsprocedure voor een mogelijke datalek in beeld

Hoofdstuk 4: Rechten van betrokkenen

Het dataveiligheidsbeleid is opgesteld als openbaar beleidsstuk en is voor iedereen beschikbaar via de website van Interzorg www.interzorgthuiszorg.nl.

4.1 Wie zijn betrokkenen?

Betrokkenen zijn personen van wie Interzorg persoonsgegevens verwerkt. Dit is bijvoorbeeld al het geval wanneer een sollicitant een open sollicitatiebrief verstuurt met daarin persoonsgegevens en Interzorg deze informatie gebruikt om contact op te nemen met de sollicitant.
Betrokkenen kunnen zijn:

- Medewerkers
- Cliënten
- Mantelzorgers, derden of anders geïnteresseerden
- Leveranciers
- Samenwerkingspartners
- Vrijwilligers

4.2 Welke rechten hebben betrokkenen?

Interzorg beschrijft duidelijk wat we met uw informatie doen en met welke doeleinden gegevens worden verwerkt.
U als medewerker, cliënt en verwerker gaat akkoord met het verwerken van gegevens.
Verwerkingen zijn vastgelegd in het verwerkingsregister.

Tevens bestaan er de volgende mogelijkheden om invloed uit te oefenen op uw data bij Interzorg:

- Het recht op dataportabiliteit: het recht om persoonsgegevens over te dragen.
- Het recht op vergetelheid: het recht om ‘vergeten’ te worden.
- Recht op inzage: het recht om de persoonsgegevens in te zien.
- Recht op rectificatie en aanvulling. het recht om de persoonsgegevens te wijzigen.
- Het recht op beperking van de verwerking: het recht om minder gegevens te laten verwerken.
- Het recht met betrekking tot geautomatiseerde besluitvorming en profilering: het recht op een menselijke blik bij besluiten.
- Het recht om bezwaar te maken tegen de gegevensverwerking.

Betrokkenen kunnen via het aanvraagformulier Dataverwerking aangeven van welk recht zij gebruik willen maken. Het formulier is voor iedereen beschikbaar op de website van Interzorg op www.interzorgthuiszorg.nl.
Het formulier stuurt men naar kwaliteit@interzorgthuiszorg.nl.
Bij ontvangst krijgt u een ontvangstbevestiging waarin aangegeven wordt dat uw verzoek binnen één maand reactie krijgt.
De reactie kan als volgt zijn:

- ❖ We gaan akkoord met het door u aangevraagd verzoek.
- ❖ We gaan ten dele akkoord met het door u aangevraagd verzoek.
- ❖ We gaan niet akkoord met het door u aangevraagd verzoek.
- ❖ Uw verzoek is dermate complex, we verzoeken u een uitstel van uiterlijk drie maanden om inhoudelijk te reageren.

Wanneer we niet of niet geheel op uw verzoek kunnen ingaan zullen we onderbouwd met motivatie toelichten waarom Interzorg niet kan voldoen aan uw verzoek.
Aan het indienen van een verzoek zijn geen kosten verbonden.

4.3 Vragen

Als u vragen hebt over uw rechten, niet tevreden bent over hoe wij hieraan uitvoering geven, of specifieke vragen heeft over de verwerking van persoonsgegevens door ons, kunt u altijd contact met ons opnemen via 0412-651428. Of per e-mail via info@interzorgthuiszorg.nl, t.a.v. Functionaris Gegevensbescherming.

Bronnen:

- B. Schermer, D. Hagenouw & N. Palot.‘ handleiding algemene verordening gegevensbescherming’ Den Haag, januari 2018
- Branchevereniging BTN. ‘privacyverklaring cliënten t.b.v. leden branchevereniging leden thuiszorg Nederland’. Houten, 18-05-2018.
- Directie Informatiebeleid – CIO. Den Haag ‘Themadossier AVG’, maart 2018
- Groep gegevensbescherming. ‘Richtlijnen inzake het recht op gegevensoverdraagbaarheid’. Brussel, 13-12-2016
- Groep gegevensbescherming. ‘Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679’. Brussel, 04-10-2017
- Groep gegevensbescherming. ‘Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO)’. Brussel, 05-04-2017.
- L.B. Sauerwein en J.J. Linnemann ‘handleiding voor het verwerken van persoonsgegevens’., Den Haag, april 2002

Links:
- https://autoriteitpersoonsgegevens.nl/ (17-05-2018)
- https://www.infosecuritymagazine.nl/wp-content/uploads/2016/10/ISM-4.pdf (17-05-2018)

Partijen ter consultatie: