Privacy beleid Amarosa

Bij Amarosa beschouwen en behandelen we alle medewerkers- en cliëntinformatie als privacygevoelig. Derhalve hebben wij de volgende Privacy missie geformuleerd :

Voor Amarosa is de bescherming van persoonsgegevens zeer belangrijk. Wij respecteren je privacy en dragen er zorg voor dat je persoonlijke gegevens altijd vertrouwelijk en in overeenstemming met de privacywetgeving worden behandeld. Wij streven er naar om de privacy van onze cliënten, bezoekers en medewerkers zo goed mogelijk te waarborgen, of het nu gaat om het vastleggen of verstrekken van gegevens, of het voeren van een vertrouwelijk gesprek met de zorgverlener.

Privacy gedragsregels

Gedragsregels geven aan hoe Amarosa wil dat zijn/haar medewerkers reageren op privacy vraagstukken en eventuele afwijkingen op het beleid. Bij het opstellen van de privacy gedragsregels zijn de zogenaamde European Fair Information Principles (FIP) gehanteerd.

Fair Information Principles zijn internationaal erkende privacy principes over hoe om te gaan met persoonsgegevens. Zij vormen het fundament voor veel (inter)nationale privacywetten, regelgeving en verdragen. De Engelstalige versie van deze principes is vermelde op de site van de OESO / OECD Privacy Guidelines.

Binnen Amarosa hanteren wij de volgende Privacy Gedragsregels:

- Als Amarosa beperken wij ons bij het verzamelen van persoonsgegevens tot enkel die gegevens die wij op wettige en rechtvaardige wijze hebben verkregen en, waar van toepassing, met de kennis of toestemming van betrokkenen. Bij persoonsgegevens kan je denken aan NAW gegevens, geboortedatum, emailadres BSN nummer, Bankrekeningnummer, medische voorgeschiedenis, medicatieoverzicht en voor medewerkers bijvoorbeeld sollicitatiebrief, cv, personeelsdossier etc.

- Als Amarosa zorgen wij ervoor dat de door ons verzamelde persoonsgegevens beperkt blijven tot de doelen waarvoor ze worden verzameld en dat ze voor die doeleinden juist, volledig en up-to-date zijn.

- Als Amarosa verzamelen we alleen persoonsgegevens nadat de doelen van het verzamelen ervan afdoende en op voorhand bekend zijn gemaakt. Het gebruik wordt beperkt tot het realiseren van deze doelen of anders (van geval tot geval

gespecificeerde) doelen die niet in strijd zijn met het doel waarvoor de gegevens eerder werden verzameld.

- Door Amarosa zullen persoonsgegevens niet openbaar worden gemaakt, beschikbaar worden gesteld of anderszins worden gebruikt voor andere doeleinden dan die gespecificeerd in punt 3. hierboven, behalve a) met instemming van de betrokkene, b) door wettelijke verplichtingen.

- Als Amarosa zorgen wij ervoor dat de aan ons ter beschikking gestelde persoonsgegevens passend worden beveiligd tegen risico's zoals verlies of ongeoorloofde toegang, vernietiging, gebruik, wijziging of openbaarmaking van gegevens.

- Als Amarosa stellen wij ons actief op en voeren wij een transparant beleid over ontwikkelingen, werkwijzen en beleidsmaatregelen met betrekking tot persoonsgegevens. Zo zijn wij helder over onze vestigingslocatie en de aard van en reden waarom wij persoonsgegevens verwerken.

- Bij Amarosa krijgt een ieder die zich daarvoor meldt : antwoord op de vraag of wij al dan niet persoonsgegevens over hem/haar hebben; binnen een redelijke termijn de beschikking over deze persoonsgegevens, tegen –indien van toepassing- een redelijke vergoeding en in een gemakkelijk leesbare vorm.
  En, indien dit verzoek aan hem/haar wordt geweigerd : een vermelding van de reden van weigering, alsmede de wijze waarop hiertegen beroep kan worden aangetekend;
  Ook kan een ieder bezwaar maken tegen de gegevens die hem/haar betreffen en heeft, als het bezwaar toegekend wordt, het recht om de gegevens te laten wissen, corrigeren, aan te vullen of te wijzigen.

- Als Amarosa zorgen wij ervoor dat wij op ieder moment in staat zijn verantwoording af te leggen over de wijze waarop wij als Organisatie invulling geven aan onze privacy gedragsregels.

- Als Amarosa zorgen wij ervoor dat de door ons verzamelde persoonsgegevens niet langer worden bewaard dan nodig voor het realiseren van het op voorhand aangegeven doel, c.q. de aangegeven doelen waarvoor de gegevens zijn verzameld.

- Als Amarosa dragen wij geen persoonsgegevens over naar landen of gebieden buiten de EER (Europese Economische Ruimte), tenzij dat land of gebied zorgt voor een passend niveau van bescherming van de rechten en vrijheden van betrokkenen met betrekking tot de verwerking van persoonsgegevens.

Bovenstaande gedragsregels zijn van toepassing op alle persoonsgegevens die Amarosa in huis heeft, verzamelt of opslaat. Dit geldt ook voor documenten die Amarosa al jaren heeft, maar niet meer gebruikt.

Amarosa informeert haar cliënten en medewerkers via privacy verklaringen, algemene voorwaarden en aanvraagformulieren. De privacy verklaringen zijn te vinden op de website https://amarosa.nl

Voor welke doelen verwerken wij persoonsgegevens?

Organisatie verwerkt persoonsgegevens uitsluitend voor zorgvuldig vastgestelde en gerechtvaardigde doeleinden. Wij verwerken jouw gegevens voor:

- Het leveren van zorg en dienstverlening
    - Opstellen en uitvoeren van de zorg- en dienstverleningsovereenkomst
    - Behandel- en begeleidingsregistraties
    - Contact en communicatie over zorg of ondersteuning
- Het voldoen aan wettelijke verplichtingen
    - Verantwoording richting gemeenten, zorgverzekeraars of zorgkantoren
    - Wettelijke administratie- en bewaarplichten
    - Verplichtingen volgens de AVG, WGBO en andere relevante wetgeving
- Organisatie en kwaliteitsverbetering
    - Verbeteren van zorgprocessen
    - Interne kwaliteitscontroles en evaluaties
- Cliënt- of medewerkerstevredenheidsonderzoeken
- Communicatie en klantencontact
    - Beantwoorden van vragen via telefoon, e-mail of website
    - Versturen van belangrijke informatie over dienstverlening
- Veiligheid en toegangsbeheer
    - Bezoekersregistratie
    - Toegangscontrole tot gebouwen of systemen
- Interne bedrijfsvoering
    - Personeelsadministratie
    - Planning en werkprocessen
    - Opleidingen en functioneringscyclus

Beveiliging persoonsgegevens

Amarosa heeft passende technische en organisatorische maatregelen getroffen om de persoonsgegevens veilig te verwerken en te bewaren. Deze maatregelen zijn in overeenstemming met de voor de zorgsector geldende beveiligingsnormen.

Om je privacy zoveel mogelijk te beschermen beperkt Amarosa het (intern) gebruik van je persoonsgegevens zoveel mogelijk.
Alleen medewerkers die op basis van hun functie je gegevens moeten gebruiken, mogen dit. Dit regelt Amarosa door middel van autorisaties in de geautomatiseerde systemen.
Amarosa heeft hiertoe een intern informatiebeveiligingsbeleid opgesteld.

Hoe gaat Amarosa operationeel om met persoonsgegevens

Voordat Amarosa persoonsgegevens gaat verwerken wordt eerst getoetst in hoeverre hier een grondslag voor is.
Amarosa verwerkt jouw persoonsgegevens alleen als aan één van de hierna genoemde voorwaarden (a t/m f) is voldaan :

- Je hebt toestemming gegeven voor de verwerking (zie ook hierboven)
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij jij partij bent, bijv. de zorg- en dienstverleningsovereenkomst
- De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting (denk hierbij aan contacten met zorgverzekeraars en bijv. financiële administratie
- De verwerking is noodzakelijk voor de bescherming van jouw vitale belangen of die van iemand anders (denk hierbij aan acuut medisch ingrijpen, bijv. bij ongeluk, noodzakelijk om medische gegevens in te zien)
- De verwerking is noodzakelijk voor de behartiging van ons eigen gerechtvaardigd belang of het gerechtvaardigd belang van een derde, behalve als jouw belangen of grondrechten en fundamentele vrijheden zwaarder wegen (bijv. registratie van bezoekers).
- De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang.

Opslaan en bewaren persoonsgegevens

Amarosa bewaart alleen de persoonsgegevens die strikt noodzakelijk zijn om haar werk te kunnen doen. Hierbij streeft Amarosa altijd naar het minimum. Persoonsgegevens van cliënten deelt Amarosa alleen met collega's die de informatie nodig hebben om hun contractueel afgesproken werkzaamheden uit te voeren. Amarosa vraagt expliciet naar die afspraken als ze persoonsgegevens met een collega wil delen. Ook houdt Amarosa zich aan de maximale bewaartermijnen.

De bewaartermijn kan per categorie gegevens en per gebruiksdoel verschillen. Meer informatie over bewaartermijnen is opgenomen in het Register van Verwerkingen. Na deze periode worden de data verwijderd of indien noodzakelijk voor archivering geanonimiseerd opgeslagen in een archief.

Specifieke regels voor verwerking van zorggegevens (WGBO)

Naast de specifieke regels voor verwerking van zorggegevens uit de WGBO gelden er onder de AVG nieuwe informatieverplichtingen en regels over het werken met toestemming van cliënten. Op grond van de AVG houdt Amarosa een register aan waarin de verwerkingsactiviteiten zijn opgenomen (het Register van Verwerkingen).

Voor de verwerking van zorggegevens is uitdrukkelijke toestemming van de betrokkene vereist, tenzij de verstrekking noodzakelijk is ter uitvoering van een wettelijk voorschrift. Ook kunnen de gegevens worden ingezien door medewerkers die de informatie moeten kunnen inzien voor de behandeling en het zorgkantoor. De persoonsgegevens worden alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht.

In het geval van verwerking van cliëntgegevens door Amarosa wordt gewerkt met een zorg- en dienstverleningsovereenkomst en/of toestemming van de cliënt.

Amarosa heeft een Privacy Officer aangesteld die de organisatie ondersteunt bij de uitvoering van het privacybeleid en de coördinatie van privacyvraagstukken. Daarnaast maakt Amarosa gebruik van een externe Functionaris Gegevensbescherming (FG). De FG houdt onafhankelijk toezicht op de naleving van de AVG, adviseert het bestuur en fungeert als contactpersoon voor de Autoriteit Persoonsgegevens. Het bestuur is als verwerkingsverantwoordelijke verantwoordelijk voor naleving van de AVG.

De rollen en verantwoordelijkheden van de Privacy Officer, de Functionaris Gegevens-bescherming en het bestuur zijn nader uitgewerkt in de rolverdeling binnen het kwaliteitsmanagementsysteem.

Gegevens verkregen bij betrokkene

Als bij de betrokkene de persoonsgegevens worden verkregen, deelt Amarosa vóór het moment van verkrijging de betrokkene het volgende mee: de identiteit van de verantwoordelijke (Amarosa) en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, tenzij de betrokkene daarvan al op de hoogte is.

Gegevens elders verkregen (niet bij betrokkene)

Als de persoonsgegevens niet rechtstreeks bij de betrokkene worden verkregen, deelt Amarosa de betrokkene op het moment van vastlegging van hem betreffende gegevens, of als de gegevens bestemd zijn voor een derde uiterlijk op het moment van de eerste verstrekking, de volgende informatie mee: de identiteit van de verantwoordelijke en de

doeleinden van de verwerking waarvoor de gegevens zijn bestemd, tenzij de betrokkene daarvan al op de hoogte is. Doel hiervan is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

Het in de vorige alinea gemelde is niet van toepassing als de mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval legt Amarosa de herkomst van de gegevens vast.

Het hierboven bepaalde is ook niet van toepassing als de vaststelling of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval moet Amarosa de betrokkene op diens verzoek informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid. Als Amarosa de betrokkene niet heeft geïnformeerd conform dit artikel, betekent dit dat de persoonsgegevens op een niet behoorlijke en op een onzorgvuldige wijze zijn verwerkt.

Het niet voldoen aan de informatieplicht kan leiden tot een onrechtmatige verwerking door Amarosa.

Delen van persoonsgegevens met een andere zorginstelling

Wanneer een cliënt overstapt naar een andere zorginstelling of wordt doorverwezen, kan Amarosa persoonsgegevens delen met de nieuwe zorgverlener. Dit gebeurt alleen wanneer dit nodig is voor goede zorgverlening en wanneer hiervoor een wettelijke basis bestaat of wanneer de cliënt hiervoor toestemming heeft gegeven. Wij delen uitsluitend de gegevens die noodzakelijk zijn voor de overdracht en gebruiken altijd beveiligde communicatiemiddelen.

Gegevens verwerken voor andere doelen

Persoonsgegevens kunnen alleen dan zonder toestemming van de betrokkene ten behoeve van wetenschappelijk onderzoek en statistiek worden verstrekt als :

- het onderzoek een algemeen belang dient
- de verwerking voor het betreffende onderzoek of de betreffende statistiek noodzakelijk is
- het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost
- bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad

Privacy by Design

Bij het ontwikkelen van nieuwe producten en diensten houdt Amarosa al in het ontwerpstadium rekening met privacy. Amarosa streeft er naar de verwerking van persoonsgegevens te beperken tot het minimaal noodzakelijke voor het nieuwe product of dienst; gegevensbescherming door ontwerp dus.

Een Privacy Impact Analyse (PIA) kan door Amarosa worden uitgevoerd indien blijkt dat er met gevoelige persoonsgegevens wordt gewerkt en de verwerking een hoog privacy risico kent.

Privacy by Default

Bij het gebruiken van de applicaties binnen Amarosa wordt er naar gestreefd de standaard-instellingen altijd zo privacy vriendelijk mogelijk te doen zijn.

Gegevensbeschermingseffectbeoordeling

Een Data Protection Impact Assessment (DPIA) of gegevensbeschermingseffectbeoordeling is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

Bij iedere nieuwe verwerking, systeemimplementatie of wezenlijke wijziging van een bestaande verwerking wordt beoordeeld of een Data Protection Impact Assessment (DPIA) verplicht is.

Een DPIA is verplicht wanneer een verwerking waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van betrokkenen, bijvoorbeeld bij grootschalige verwerking van bijzondere persoonsgegevens.

Deze beoordeling wordt vastgelegd. Indien sprake is van een hoog privacyrisico, wordt voorafgaand aan de implementatie een DPIA uitgevoerd. Zonder vastgelegde privacybeoordeling vindt geen implementatie plaats.

Rechten van betrokkenen

Onder de AVG hebben betrokkenen de volgende rechten :

- het recht op transparante informatie. Je hebt het recht om te weten of, en zo ja welke persoonsgegevens wij verwerken en waarom we dat doen.
- het recht op inzage en afschrift van je persoonsgegevens
- het recht op rectificatie van de persoonsgegevens (corrigeren, aanvullen)
- het recht op het beperken van gebruik van de persoonsgegevens

- het recht op wissen, verwijderen, vernietigen van je persoonsgegevens (recht om vergeten te worden).
- Het recht op data portabiliteit (het recht om persoonsgegevens over te dragen)
- Het recht op bezwaar

Amarosa laat je zo snel mogelijk, maar in ieder geval binnen één maand na ontvangst van je verzoek schriftelijk weten of en in hoeverre ze aan je verzoek voldoet. Als Amarosa aan je verzoek voldoet voert zij dit binnen één maand na ontvangst van het verzoek uit.

Cameratoezicht

Om de veiligheid van bewoners, bezoekers en medewerkers te waarborgen, maakt Amarosa gebruik van cameratoezicht in en rondom de gebouwen.

- De camera's zijn duidelijk zichtbaar geplaatst en worden uitsluitend ingezet voor beveiligingsdoeleinden.
- De beelden worden alleen bekeken bij incidenten of wanneer dit noodzakelijk is voor de veiligheid.
- Camerabeelden worden maximaal 31 dagen bewaard, tenzij ze nodig zijn voor een onderzoek of juridische procedure.
- Alleen daartoe bevoegde medewerkers hebben toegang tot de beelden.
- Cameratoezicht vindt plaats conform de wettelijke bepalingen van de Algemene Verordening Gegevensbescherming (AVG).

Datalekken

Amarosa heeft een proces ingericht dat het melden en afhandelen van datalekken volgt. Een datalek wordt ALTIJD geregistreerd na melding. Dit gebeurt in SmartManSys, het management kwaliteitssysteem.

Na beoordeling of het datalek mogelijk schadelijke gevolgen heeft voor de betrokkene(n) wordt bij negatieve impact ook melding gedaan bij de Autoriteit Persoonsgegevens (AP). Indien van toepassing wordt ook melding aan de betrokkene(n) gedaan. De beoordeling van de meldplicht wordt uitgevoerd door de CISO in samenwerking met de Privacy Officer. De verwerkingsverantwoordelijke (bestuur/directie) besluit op basis van dit advies over melding aan de Autoriteit Persoonsgegevens en/of betrokkenen.

Tot slot wordt elk geconstateerd datalek beoordeeld. Indien noodzakelijk wordt er een traject opgestart om te voorkomen dat een datalek opnieuw plaatsvindt. Denk hierbij aan maatregelen die procesmatig moeten worden aangepast, maar ook technisch of organisatorisch moeten worden opgevolgd. De privacy functionaris begeleidt de opvolging en wordt op de hoogte gehouden.

Overzicht bevoegdheden en verantwoordelijkheden

De verantwoordelijkheden voor signalering, coördinatie, advisering, besluitvorming en vastlegging zijn uitgewerkt in een afzonderlijke rolverdeling binnen het kwaliteitsmanagementsysteem (hoofdstuk 1.4). Het bestuur is als verwerkings-verantwoordelijke eindverantwoordelijk voor naleving van dit privacybeleid.