



Privacy

Hoe gaat Aveleijn om met Privacy

Eigenaar: Raad van Bestuur
Auteur: Hans Kompanje, functionaris gegevensbescherming a.i. (fg@aveleijn.nl)
Datum: 14 juni 2018
Versie: 3.0

Inhoudsopgave

1	Referenties	4
1.1	<i>Begrippenkader</i>	4
1.2	<i>Wettelijk kader</i>	5
2	Over Aveleijn	6
2.1	<i>Missie, visie en kernwaarden</i>	6
2.2	<i>Ontmoeten</i>	6
2.3	<i>Ontwikkelen</i>	6
2.4	<i>Ondersteunen</i>	6
2.5	<i>Strategie</i>	7
3	Persoonsgegevens	8
3.1	<i>Reikwijdte</i>	8
3.2	<i>Doel</i>	8
3.3	<i>Vertegenwoordiging</i>	8
3.4	<i>Voorwaarden voor rechtmatige verwerking</i>	8
3.5	<i>Kader voor het verwerken van persoonsgegevens</i>	8
3.6	<i>Opslaan van persoonsgegevens</i>	9
3.7	<i>Bewaren van persoonsgegevens</i>	9
3.8	<i>Specifieke regels voor verwerking van zorggegevens (WGBO)</i>	10
3.9	<i>Informatieverstrekking aan betrokkene</i>	10
3.10	<i>Gegevens elders verkregen (niet bij de betrokkene)</i>	11
3.11	<i>Gegevens verwerken voor andere doelen</i>	11
3.12	<i>Privacy by Default</i>	11
3.13	<i>Privacy by Design</i>	12
3.14	<i>Melden en informeren</i>	12
3.15	<i>Wetenschappelijk onderzoek en/of statistiek</i>	12
4	Rechten van de betrokkenen	13
4.1	<i>Inzagerecht</i>	13
4.2	<i>Correctierecht</i>	13
4.3	<i>Verwijderrecht</i>	13
4.4	<i>Recht van verzet</i>	13
4.5	<i>Het recht op dataportabiliteit</i>	14
4.6	<i>Het recht op informatie</i>	14
4.7	<i>Uitwisselen van informatie</i>	14
5	Datalekken	15
5.1	<i>Proces datalekken</i>	15
5.2	<i>Datalekken register</i>	15
5.3	<i>Opvolging</i>	15

6	Functionaris Gegevensbescherming	16
6.1	<i>Rol FG</i>	16
6.2	<i>Awareness en training</i>	16
7	Het verwerken van gegevens	17
8	Overzicht verwerkingen	18
8.1	<i>Bewaartermijnen</i>	18
8.2	<i>Activiteiten als gevolg van de implementatie van het informatiebeveiligingsbeleid</i>	18
9	Gekoppelde processen	19
9.1	<i>Datalek proces</i>	19
9.2	<i>Inzage, correctie en verwijderrecht</i>	19
9.3	<i>Informatieverstrekking aan de betrokkene</i>	19
9.4	<i>Recht op inzage en afschrift van opgenomen persoonsgegevens</i>	19
9.5	<i>Recht op verbetering, aanvulling, verwijdering of afscherming</i>	19
9.6	<i>Toegangscontrole en bezoekersregistratie</i>	20
9.7	<i>Social Media beleid</i>	20
9.8	<i>Camera gebruik</i>	20

1 Referenties

1.1 Begrippenkader

In onderstaand overzicht worden de begrippen gebruikt in dit document kort uitgelegd:

Persoonsgegeven	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon
Zorggegevens	Persoonsgegevens die direct of indirect betrekking hebben op de lichamelijke of de geestelijke gesteldheid van betrokkenen, verzameld door een beroepsbeoefenaar op het gebied van de gezondheidszorg in het kader van zijn beroepsuitoefening
Verwerking van persoonsgegevens	Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens
Verstrekken van persoonsgegevens	Bekend maken of ter beschikking stellen van gegevens.
Verzamelen van persoonsgegevens	Het verkrijgen van persoonsgegevens.
Bestand	Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen
Verantwoordelijke	De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt
Verwerker	Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft
Derde	Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken
Ontvanger	Degene aan wie de persoonsgegevens worden verstrekt
Toestemming van de betrokkene	Elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.
Autoriteit Persoonsgegevens (AP)	Het AP bedoeld in de WBP, dat tot taak heeft toe te zien op de verwerking van persoonsgegevens
Klachtenfunctionaris	De functionaris die binnen Aveleijn bemiddelt bij klachten die zijn ingediend door cliënten, verwanten of derden. De klachtenfunctionaris is ingesteld in het kader van de Wet kwaliteit, klachten en geschillen zorg.
WBP	Wet Bescherming Persoonsgegevens van 6 juli 2000, Stb. 302, houdende regels inzake de bescherming van persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming, de vervanger van de WBP per 25 mei 2018
WGBO	Wet op de geneeskundige behandelingsovereenkomst van 17 november 1994, Stb. 837, tot wijziging van het Burgerlijk Wetboek en enige andere wetten in verband met de opnemings van bepalingen omtrent de overeenkomst tot het verrichten van handelingen op het gebied van de geneeskunst, laatstelijk gewijzigd bij wet van 28 januari 1999, Stb. 30

1.2 Wettelijk kader

Het privacy beleid kan worden herleid tot een aantal wereldwijd geaccepteerde privacy beginselen. Die vormen de basis voor nationale en internationale regels. Deze regels zijn te vinden in algemene wetgeving en als onderdeel van specifieke wetten. Hieronder een kleine selectie.

- OECD Privacy Framework 2013
- Verdrag 108 Raad van Europa 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens;
- Handvest van de grondrechten van de Europese Unie (artikel 7 en 8); Grondwet (artikel 10);
- Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (tot 25 mei 2018, dit is de vigerende Europese privacyrichtlijn);
- Interpretaties van Richtlijn 95/46/EG als verwoord door de zogenaamde artikel 29 werkgroep (Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens-WP 29) en gepubliceerd op hun website http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm;
- Wet bescherming persoonsgegevens (tot 25 mei 2018) (Stb. 2000, 302);
- Richtlijn 2002/58/EG gewijzigd door 2009/136/EG (ePrivacy richtlijn);
- Telecommunicatiewet (Wet van 19 oktober 1988, houdende regels inzake de telecommunicatie);
- Wet op de Ondernemingsraden;
- Wetten met impact op gegevensverwerking (zoals de Wet op de Geneeskundige behandelingsovereenkomst, artikel 7:446-468 BW);
- Verordening (EU) 2016/679 ('AVG') betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (vanaf 25 mei 2018).
- Wet op de geneeskundige behandelingsovereenkomst (WGBO);
- Wet kwaliteit, klachten en geschillen zorg (Wkkgz);
- Wet op de beroepen in de individuele gezondheidszorg (Wet BIG);
- Zorgverzekeringswet (Zvw);
- Wet marktordening gezondheidszorg (Wmg);
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

2 Over Aveleijn

2.1 Missie, visie en kernwaarden

Aveleijn zet zich in voor een leven vol betekenis voor iedereen. Hierbij gaan we uit van de eigen kracht van de cliënt en het onderzoeken, ontplooien en aanspreken van eigen dromen, wensen en talenten. De kernwaarden Ontmoeten, Ontwikkelen en Ondersteunen zijn hierbij richtinggevend en maken ons uniek.

2.2 Ontmoeten

Om aansluiting te vinden bij de leef- en belevingswereld van onze cliënten willen we elkaar écht leren kennen. Onvoorwaardelijke aandacht geven, waarbij we uitgaan van de unieke mens. Ruimte bieden voor de dialoog en gelijkwaardige communicatie met elkaar. We zoeken oprechte verbindingen en open samenwerking met cliënten, verwanten en professionals om uit te kunnen gaan van ieders eigen kracht.

2.3 Ontwikkelen

Aveleijn ondersteunt cliënten en hun netwerk bij de ontwikkelingsstappen. Hoe klein of groot ook. We hebben oog en aandacht voor ontwikkeling in brede zin. Persoonlijke ontwikkeling van cliënten en medewerkers, kennisontwikkeling, de doorontwikkeling van onze organisatie en vernieuwingen in de zorg hangen daarbij nauw samen.

2.4 Ondersteunen

Aveleijn beschikt over een integraal, breed zorgaanbod om cliënten in alle levensfasen ondersteuning te kunnen bieden. We creëren ruimte voor de ontwikkeling van een eigen identiteit en helpen onze cliënten naar vermogen deel te nemen aan de maatschappij.

Onze medewerkers zijn van nature (maatschappelijk) betrokken professionals met een passie voor mensen, zowel voor cliënten als collega's. We realiseren ons hoezeer kwaliteit van arbeid en kwaliteit van ondersteuning samen op gaan. Binnen het waardenprogramma staan we dan ook met elkaar stil bij ons vak en de manier waarop onze kernwaarden invulling krijgen in de dagelijkse praktijk.

Aveleijn investeert in professionele ontwikkeling en echte samenwerking met alle betrokkenen binnen en buiten Aveleijn, waarbij reflectie in praktijk de basis vormt. Door vragen te blijven stellen en stil te staan bij wat goed gaat, beter kan, dilemma's en handelingen die het verschil maken, werken we continu aan het waarborgen van onze kwaliteit van zorg.

2.5 Strategie

Bij Aveleijn beschouwen en behandelen we alle medewerkers- en cliëntinformatie als privacygevoelig. Verwerking van privacygevoelige informatie kan leiden tot een inbreuk op de persoonlijke levenssfeer en is daarom gebonden aan strikte regels. Om ervoor te zorgen dat we de regels naleven, hanteren we een aantal normen. Deze normen zijn van toepassing op alles wat we doen met privacygevoelige informatie. Ze zijn van toepassing op alle persoonsgegevens die we in huis hebben, verzamelen of opslaan. Dit geldt ook voor documenten die we al jaren hebben, maar niet meer gebruiken.

1. We verwerken privacygevoelige informatie alleen voor een gerechtvaardigd en vooraf vastgesteld doel, zoals behandeling.
2. We verwerken alleen de privacygevoelige informatie die nodig is voor het vooraf vastgestelde doel en alleen gedurende de strikt noodzakelijke periode.

We bewaren alleen de privacygevoelige informatie die strikt noodzakelijk is om ons werk te kunnen doen. Hierbij streven we altijd naar het minimum. Privacygevoelige informatie van cliënten delen we alleen met collega's die de informatie nodig hebben om hun contractueel afgesproken werkzaamheden uit te voeren. We vragen expliciet naar die afspraken als we privacygevoelige informatie met een collega willen delen. We houden ons aan de maximale bewaartermijnen. De bewaartermijn kan per categorie gegevens en per gebruiksdoel verschillen. Meer informatie over bewaartermijnen is opgenomen in het document bewaartermijnen.

3. We verwerken privacygevoelige informatie alleen als de klant daarover vooraf is geïnformeerd.

We informeren onze klanten onder andere via privacy statements, algemene voorwaarden en aanvraagformulieren. Onze privacy statements zijn te vinden op www.Aveleijn.com/privacy.

We maken ons beleid kenbaar op verschillende fronten. Via onze externe website is een uitgebreide versie te zien waarin wordt beschreven hoe wij met privacy omgaan en wat wij doen om te garanderen dat persoonlijke informatie vertrouwelijk en integer wordt behandeld.

Intern hebben wij procedures rondom het gebruik van persoonsgegevens. Dit geldt voor zowel de personeelsgegevens, als de cliëntgegevens.

3 Persoonsgegevens

3.1 Reikwijdte

Dit reglement is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een digitaal bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

3.2 Doel

Het doel van dit reglement is een praktische uitwerking te geven van de bepalingen van de AVG en, voor zover van toepassing, de bepalingen van de WGBO. Dit reglement wordt gebruikt binnen Aveleijn en heeft betrekking op het door Aveleijn op te stellen overzicht van genoemde verwerkingen van persoonsgegevens. Dit overzicht vormt één geheel met dit reglement. Binnen de doelstelling van dit reglement zullen geen andere gegevens worden opgenomen dan onder artikel 3.1 omschreven.

3.3 Vertegenwoordiging

Als de betrokkene minderjarig is en nog geen zestien jaar is, is in de plaats van de toestemming van de betrokkene de toestemming van zijn wettelijk vertegenwoordiger vereist. Hetzelfde geldt als de betrokkene onder curatele is gesteld of als ten behoeve van de betrokkene een mentorschap is ingesteld of als de betrokkene niet in staat is om zijn wil te bepalen. Als de betrokkene 16 jaar of ouder is en in staat is tot een redelijke waardering van zijn belangen, treedt de betrokkene zelf op. Binnen Nederland is voor vertegenwoordiging de volgende onderverdeling gemaakt :

Kind is jonger dan 12 jaar -> Ouders/Voogd

Kind is tussen de 12 en 16 jaar -> Zowel kind als Ouders/voogd

Kind is ouder dan 16 jaar -> Kind

3.4 Voorwaarden voor rechtmatige verwerking

Persoonsgegevens worden in overeenstemming met dit reglement en de wet op behoorlijke en zorgvuldige wijze verwerkt en niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.

De verantwoordelijke is verantwoordelijk voor het goed functioneren van de verwerking van persoonsgegevens; voor het verwerken van persoonsgegevens is dit bijvoorbeeld de afdeling personeelsadministratie. Zijn/ haar handelwijze met betrekking tot de verwerking van de persoonsgegevens wordt bepaald door dit beleidsdocument. De verantwoordelijke is aansprakelijk voor de eventuele schade als gevolg van het niet naleven van dit beleid.

De verantwoordelijke draagt er zorg voor dat passende technische en organisatorische maatregelen worden uitgevoerd ter beveiliging tegen verlies of enige vorm van onrechtmatige verwerking. De maatregelen die Aveleijn heeft genomen zijn beschreven in het informatieveiligheidsbeleid. De verantwoordelijke is niet aansprakelijk als hij kan aantonen dat de betreffende onrechtmatigheid hem niet kan worden toegerekend. De verantwoordelijke ziet toe op de naleving van de beveiligingsmaatregelen.

3.5 Kader voor het verwerken van persoonsgegevens

Voordat we persoonsgegevens gaan verwerken wordt eerst getoetst in hoeverre hier een grondslag voor is. Dit wordt getoetst aan de volgende zes opties:

- **Toestemming:** De betrokkene (dit is degene op wie de gegevens betrekking hebben) heeft voor de verwerking zijn **ondubbelzinnige toestemming** gegeven voor de verwerking van zijn gegevens voor één of meerdere doelen. (Bijvoorbeeld bewaren CV.)
- **Uitvoering overeenkomst:** De gegevensverwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkenen en die noodzakelijk zijn voor het sluiten van een overeenkomst. (Bijvoorbeeld aanschaf product via website, adresgegevens nodig voor verzending.)
- **Wettelijke verplichting:** De gegevensverwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting** van de verantwoordelijke. (Bijvoorbeeld HR administratie.)
- **Vitaal belang:** De gegevensverwerking is noodzakelijk om de **vitale belangen** van de betrokkene of van een andere natuurlijke persoon te beschermen. Hierbij valt de te denken aan acuut medisch ingrijpen. (Bijvoorbeeld bij ongeluk, noodzakelijk om medische gegevens in te zien.)
- **Algemeen belang:** de verwerking is noodzakelijk voor de vervulling van een taak van **algemeen belang** of van een taak in het kader van de **uitoefening van het openbaar gezag** dat aan de verwerkingsverantwoordelijke is opgedragen. (Bijvoorbeeld nodig bij gedelegeerd belang vanuit wetgeving, toezicht.)
- **Gerechtvaardigd belang:** de verwerking is noodzakelijk voor de behartiging van de **gerechtvaardigde belangen** van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. (Bijvoorbeeld registratie van bezoekers.)

3.6 Opslaan van persoonsgegevens

We denken na voordat we persoonsgegevens opslaan. Bij het gebruik van persoonsgegevens wordt eerst onderzocht of deze gegevens noodzakelijk zijn. Indien niet noodzakelijk voor het doel, worden de gegevens niet opgeslagen. Soms komen we er niet onderuit. Bijvoorbeeld wettelijk worden wij verplicht om bepaalde gegevens te bewaren en op te slaan. Dit doen we volgens de wettelijke normen die zijn genoemd in ons informatie beveiligingsbeleid.

3.7 Bewaren van persoonsgegevens

Persoonsgegevens worden alleen bewaard als hier noodzaak voor is. Dit kan een wettelijke verplichting zijn, of noodzakelijk voor de uitvoer van de overeenkomst. Voor het bewaren van deze gegevens houden we aan bewaartermijnen, die zijn beschreven in een apart document. Hierin wordt per soort data beschreven hoe lang we minimaal en maximaal de data bewaren. Nadat deze periodes zijn verlopen wordt de data verwijderd, of indien noodzakelijk voor archivering geanonimiseerd opgeslagen in een archief.

3.8 Specifieke regels voor verwerking van zorggegevens (WGBO)

Onder de AVG gelden er nieuwe informatieverplichtingen en nieuwe regels over het werken met toestemming van cliënten. Aveleijn houdt op grond van de AVG een register bij met verwerkingsactiviteiten (het verwerkingsregister). Ook onderzoeken we de gevolgen voor privacy van medewerkers en cliënten als we processen wijzigen (denk bijvoorbeeld aan het implementeren van nieuwe ICT programma's) en hebben we een Functionaris Gegevensbescherming (FG) aangesteld, die intern toetst of Aveleijn zorgvuldig met persoonsgegevens omgaat.

Voor 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 cliënt gegevens door Aveleijn wordt gewerkt met een zorg-en dienstverleningsovereenkomst en/of toestemming van de cliënt.

Een schriftelijke (waaronder digitale) vastlegging van de toestemming van de cliënt (bijvoorbeeld in het medisch dossier) is noodzakelijk. Als de toestemming voor verwerking van cliëntgegevens reeds vóór inwerkingtreding van de AVG is verleend, dient binnen twee jaar vanaf inwerkingtreding van de AVG (25 mei 2018) te worden getoetst of die toestemming in overeenstemming met de strengere voorschriften van de AVG is verkregen. Alleen dan is het opnieuw vragen van toestemming niet vereist.

Onder de AVG moet Aveleijn kunnen aantonen dat de cliënt toestemming heeft gegeven voor de verwerking van zijn of haar gegevens. Deze verplichting komt voor een groot deel overeen met de registratieplicht voor toestemming die in de Wet cliëntenrechten bij elektronische verwerking van gegevens is opgenomen.

De Wet cliëntenrechten bij elektronische verwerking van gegevens regelt dat elektronische inzage per 1 juli 2020 kosteloos moet zijn. De AVG bepaalt dat uw cliënt deze inzage vanaf 25 mei 2018 al kosteloos moet kunnen krijgen, al dan niet elektronisch.

3.9 Informatieverstrekking aan betrokkene

Voor de rechten van de betrokkene is het noodzakelijk te beschrijven hoe de informatie met de betrokkene gedeeld kan worden en op welke manier. Hieronder wordt beschreven wat hiervoor noodzakelijk is. Dit wordt verder uitgewerkt in processen binnen de betrokken afdelingen.

Een betrokkene heeft bij verwerking van zijn of haar persoonsgegevens recht op:

- transparante informatie en communicatie;
- inzage en rectificatie;
- verwijdering ('recht op vergetelheid');
- beperking van de verwerking;
- overdraagbaarheid van gegevens ('dataportabiliteit');
- het maken van bezwaar;
- niet te worden onderworpen aan geautomatiseerde individuele besluitvorming, waaronder profilering.

Als bij de betrokkene de persoonsgegevens worden verkregen, deelt de verantwoordelijke vóór het moment van verkrijging de betrokkene het volgende mee:

- de identiteit van de verantwoordelijke (Aveleijn) en
- de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, tenzij de betrokkene daarvan al op de hoogte is.

Dit is noodzakelijk om transparantie naar de cliënt aan te geven rondom het gebruik van de persoonsgegevens.

De betrokkene verstrekt nader informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

3.10 Gegevens elders verkregen (niet bij de betrokkene)

Als de persoonsgegevens niet rechtstreeks bij de betrokkene worden verkregen, deelt de verantwoordelijke 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.

De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

Dit is niet van toepassing als de mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval legt de verantwoordelijke de herkomst van de gegevens vast. Het bepaalde onder 3.2 is ook niet van toepassing als de vaststelling of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval moet de verantwoordelijke de betrokkene op diens verzoek informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid. Als de verantwoordelijke 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 leidt tot een onrechtmatige verwerking. Zie ook 3.5.

3.11 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 en
- bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad

3.12 Privacy by Default

Bij het verwerken van data houden we ons aan de opgestelde normen. Niet onnodig informatie verwerken en alleen gebruiken en bewaren wat noodzakelijk is voor het doel. Niet meer en niet minder. Op deze manier beperken we mogelijke fouten en kunnen wij open en transparant aangeven welke gegevens wij bewerken. Bij het gebruiken van de applicaties binnen Aveleijn worden de applicaties zo ingesteld dat het verwerken van persoonsgegevens wordt geminimaliseerd tot het hoogst noodzakelijke en de meest privacy vriendelijke stand. Daarnaast wordt de toegang tot

privacygevoelige data beperkt en wordt alleen toegang verleend aan personen die deze toegang nodig hebben. Geen onnodige toegang dus. Daarnaast wordt de data alleen bewaard indien dit ook noodzakelijk is.

3.13 Privacy by Design

Indien er nieuwe producten of diensten worden ontwikkeld, houden we bij de start van een traject rekening met het minimaal verwerken van persoonsgegevens. Een Privacy Impact Analyse wordt uitgevoerd indien blijkt dat er met persoonsgegevens wordt gewerkt.

3.14 Melden en informeren

Voordat we starten met het verwerken van persoonsgegevens zorgen we dat de betrokkenen zijn geïnformeerd. We melden wat we verwerken en hoe we dit doen. Dit gebeurt op de website, door dit kenbaar te maken via een privacy statement, bij medewerkers tijdens het aannamebeleid en bij patiënten tijdens de intake.

3.15 Wetenschappelijk onderzoek en/of statistiek

Een verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden mag worden uitgevoerd mits dit is onderworpen aan passende waarborgen in overeenstemming met de wetgeving. Dit houdt in dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van minimale gegevensverwerking te garanderen. Een maatregel is pseudonimisering of anonimisering van de persoonsgegevens.

4 Rechten van de betrokkenen

Een betrokkene heeft een aantal rechten die zijn gedefinieerd door de wetgever. In onderstaand overzicht worden deze rechten globaal beschreven.

4.1 Inzagerecht

Het inzagerecht is van toepassing voor alle cliënten. Binnen Aveleijn wordt een proces beschreven hoe hiermee om wordt gegaan. Een betrokkene kan het verzoek indienen om inzage in zijn/haar eigen persoonlijke data die is verwerkt door Aveleijn. Indien het een kind jonger is dan 16 jaar is, wordt dit verzoek mede gedaan door een wettelijk vertegenwoordiger of ouder. Het betreft informatie in het dossier en eventuele correspondentie. De betrokkene kan zelf kennismaken van de informatie die over hem of haar wordt opgeslagen.

Om dit recht mogelijk te maken moet de identiteit van de aanvrager worden gecontroleerd. Aveleijn kan de betrokkene inzage geven in de persoonsgegevens door een kopieën of afdrukken te overhandigen of inzage ter plekke. Het recht op inzage kan worden geweigerd als dit in het belang is van de bescherming van de persoonlijke levenssfeer van een ander persoon. Als voorbeeld, indien het niet mogelijk is om de informatie van de betrokkene te laten zien zonder ook gevoelige informatie van een andere betrokkene weer te geven, bijvoorbeeld in een verslag waar van meerdere cliënten informatie is beschreven, wordt dit niet getoond.

4.2 Correctierecht

Cliënten hebben het recht om hun gegevens te laten corrigeren indien deze naar hun mening niet juist zijn. Ze mogen vragen om de gegevens te verbeteren, aan te vullen, verwijderen of af te schermen.

Iemand kan om correctie vragen als zijn persoonsgegevens:

- feitelijk onjuist zijn;
- onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld;
- op een andere manier in strijd met een wet worden gebruikt.

De betrokkene kan vragen om correctie van op hem betrekking hebbende gegevens als deze feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn, of in strijd met een wettelijk voorschrift, in de verwerking voorkomen. De weigering moet worden aangegeven met gegronde redenen.

4.3 Verwijderrecht

De betrokkene kan vragen om vernietiging van op hem betrekking hebbende gegevens indien deze feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn, of in strijd met een wettelijk voorschrift. Binnen 4 weken na ontvangst van het schriftelijke verzoek wordt aangegeven of hieraan voldaan kan worden.

Aveleijn vernietigt de gegevens binnen drie maanden na het verzoek van de betrokkene, tenzij redelijkerwijs aannemelijk is dat het toch bewaren van aanmerkelijk belang is voor een ander dan de betrokkene, alsmede voor zover bewaring op grond van een wettelijk voorschrift vereist is.

4.4 Recht van verzet

Een betrokkene heeft het recht aan een organisatie te vragen hun persoonsgegevens niet meer te gebruiken. Dit heet het recht van verzet. Dit is bijvoorbeeld van toepassing als de organisatie persoonsgegevens gebruikt voor marketingdoeleinden. Ten tweede kan iemand ook om bijzondere persoonlijke redenen van het recht van verzet gebruikmaken.

De betrokkene heeft het recht om vanwege een specifieke situatie bezwaar te maken tegen de verwerking van persoonsgegevens. Aveleijn is dan verplicht om de verwerking te stoppen, tenzij er gronden zijn die voor de verwerker zwaarder wegen dan de vrijheid van de betrokkene.

4.5 Het recht op dataportabiliteit

Dataportabiliteit wordt in de wetgeving 'gegevensoverdraagbaarheid' genoemd. Dit recht houdt in dat betrokkenen die toestemming hebben gegeven voor de verwerking van hun persoonsgegevens, de verantwoordelijke kunnen vragen om deze gegevens door te sturen. Je bent als verantwoordelijke verplicht om deze gegevens op verzoek van de betrokkene rechtstreeks naar een andere organisatie te sturen. Als dat niet mogelijk is, wordt de data in een gangbaar bestandsformaat aangeleverd bij de aanvrager, zodat het geïmporteerd kan worden bij andere aanbieders.

4.6 Het recht op informatie

De verantwoordelijke is verplicht om de betrokkene te informeren over de verwerking van zijn of haar persoonsgegevens. Deze informatie is te vinden op het privacy statement op de website. Hierin wordt informatie weergegeven rondom de bewaartermijn van de gegevens, de toegankelijkheid, beveiligingsmethodes en de contactgegevens van de FG.

4.7 Uitwisselen van informatie

De verantwoordelijke wisselt informatie uit met 3^e partijen, zoals leveranciers en partners. Voor alle uitwisselingen geldt dat deze informatie alleen uitgewisseld mag worden als in een verwerkersovereenkomst is beschreven wat voor persoonlijke informatie dit is en wat de technische en organisatorische maatregelen zijn die zijn genomen om aan te kunnen tonen dat de 3^e partij veilig omgaat met persoonsgegevens van Aveleijn.

5 Datalekken

5.1 Proces datalekken

Aveleijn heeft een proces ingericht dat het melden en afhandelen van datalekken volgt. Een datalek wordt **ALTIJD** geregistreerd na melding. Dit gebeurt in het datalekken register, wat op een SharePoint lijst wordt bijgehouden. Na beoordeling of het datalek mogelijke schadelijke gevolgen heeft voor de betrokkene(n) wordt bij schade ook melding gedaan bij de Autoriteit Persoonsgegevens. Indien van toepassing wordt ook melding gedaan bij de betrokkene(n) over het datalek.

5.2 Datalekken register

In het datalekken register wordt bijgehouden welke datalekken binnen de organisatie zijn gemeld. Daarnaast wordt geregistreerd wie de melding heeft gedaan, om wat voor soort data het gaat en wat de opvolging is van het geconstateerde lek.

5.3 Opvolging

Elk geconstateerd datalek wordt beoordeeld. Indien noodzakelijk wordt er een traject opgestart om te voorkomen dat een datalek opnieuw plaatsvindt. Dit kunnen maatregelen zijn die procesmatig moeten worden aangepast, maar ook technisch of organisatorisch wordt opgevolgd. De FG begeleidt de opvolging en wordt hierover op de hoogte gehouden.

Voor meer informatie, raadpleeg de procedure melden datalekken.

6 Functionaris Gegevensbescherming

Vanuit Europese wetgeving is vanaf april 2016 de Algemene Verordening Gegevensbescherming (AVG) effectief. Binnen deze wetgeving is een rol van Functionaris Gegevensbescherming (FG) benoemd. Elke organisatie die op grote schaal (bijzondere) persoonsgegevens verwerkt is verplicht deze rol binnen de organisatie te benoemen. Aveleijn beschikt over een FG. Deze functionaris is te bereiken op fg@aveleijn.nl. Belangrijk is de onafhankelijkheid van de FG. De FG rol rapporteert rechtstreeks aan de Raad van Bestuur en heeft hier ook directe lijnen mee. Binnen Aveleijn volstaat het om één FG aan te duiden, op voorwaarde dat deze voor elke vestiging makkelijk bereikbaar is.

6.1 Rol FG

De Functionaris Gegevensbescherming (FG) voert de werkzaamheden onafhankelijk uit en ontvangt hierbij geen instructies vanuit de organisatie.

Op basis van de AVG worden volgende taken aan de FG toebedeeld:

- Het geven van informatie en advies naar medewerkers over de toepassing van de AVG;
- Het toezien op naleving van alle privacy regelgeving;
- Toezien op het naleven van het beleid van de verantwoordelijke of bewerkster, met inbegrip van de toewijzing van verantwoordelijkheden;
- Creëren van bewustwording en begeleiden bij opleidingen bij het verwerken van privacygevoelige data;
- Het faciliteren van audits;
- Het geven van antwoord op vraagstukken met betrekking tot gegevensverwerking en rechten van de betrokkene wiens data wordt verwerkt;
- Gevraagd en ongevraagd advies verstrekken over gegevensbescherming;
- Met de autoriteit persoonsgegevens samenwerken;
- Optreden als contactpunt voor de autoriteit persoonsgegevens.

Bij de uitvoering van deze taken houdt de FG rekening met het aan verwerkingen verbonden risico's, en met de aard, de omvang, de context, volledigheid en nauwkeurigheid van gegevens en de verwerkingsdoeleinden. Dit gebeurt op een onafhankelijke wijze en met betrekking tot elke verwerking van gegevens binnen de onderneming, waaronder onder meer de HR, marketing en IT-departement vallen. Verder is hij betrokken bij de uitwerking van een 'Information Security Policy', of privacy beleid, en het veiligheidsplan. Met behulp van gepaste technische en organisatorische maatregelen beschermt de FG persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.

De classificatie en het beheer van de gevoelige gegevens, waarbij gegevensstromen en mogelijke risico's in kaart worden gebracht, is het startpunt van waaruit de FG de gegevensbescherming verzekert. De bescherming beperkt zich niet tot een fysieke beveiliging van gegevens, ook medewerkers gerelateerde veiligheid en logische toegangsbeveiliging vallen onder zijn toezicht. Periodieke audits en compliance checks met de alsmaar veranderende systemen en wetgevingen zijn hierbij noodzakelijk.

6.2 Awareness en training

Elke medewerker krijgt bij indiensttreding documentatie overhandigd hoe om te gaan met privacy en persoonsgegevens.

7 Het verwerken van gegevens

Binnen Aveleijn houden we de volgende 10 punten aan. Doel hiervan is het correct verwerken van persoonsgegevens. We streven de volgende doelstellingen na:

1. We zijn transparant over de persoonsgegevens die worden verwerkt en het verwerkingsdoel, zowel naar de betrokkene als naar de toezichthouder. De gevoerde communicatie is eerlijk, eenvoudig toegankelijk en begrijpelijk. Het transparantieprincipe is ook van toepassing wanneer de persoonsgegevens worden uitgewisseld.
2. We verwerken enkel de gegevens die relevant zijn voor het uitvoeren van de taken. Elke taak waarbij persoonsgegevens worden verwerkt, is rechtmatig. Dit betekent onder meer dat de verwerking in overeenstemming is met de missie en kernwaarden van Aveleijn. Dit wordt telkens geëvalueerd bij een nieuw verwerkingsdoel, waardoor we privacy by design toepassen.
3. We verwerken enkel de persoonsgegevens die strikt noodzakelijk voor de uitvoering van de activiteiten.
4. We zien toe op de integriteit van de persoonsgegevens gedurende de gehele verwerkingscyclus.
5. We bewaren gegevens niet langer dan noodzakelijk. De noodzakelijkheid is gecontroleerd tegenover wettelijke verplichtingen en de rechten en vrijheden van de betrokkene.
6. We voorkomen inbreuken die voortvloeien uit het verwerken van persoonsgegevens. Informatieveiligheid, gegevensbescherming bij ontwerp en privacy-vriendelijke standaardinstellingen zijn hiervoor hulpmiddelen. Wanneer een inbreuk plaatsvindt, wordt hierover gerapporteerd in lijn met de regelgeving ter zake.
7. We zijn in staat om alle geldende rechten van een betrokkene, zoals het recht op inzage, afschrift en eventueel ook schrapping uit te voeren. Aveleijn bewaakt hierbij over de eventuele beperkingen die op deze rechten van toepassing zijn.
8. We waken er actief over dat bij het verwerken van de persoonsgegevens voor een welbepaald doel, de rechten en vrijheden (bijvoorbeeld recht op verzekeraarbaarheid, recht op zorg) van de betrokkene ge vrijwaard blijven.
9. We verwerken gegevens in lijn met de rechten en vrijheden die gelden in de Europese Economische Ruimte en controleert de toepassing hiervan wanneer de gegevens worden uitgewisseld daarbuiten. Aveleijn leeft bijgevolg alle wettelijke en normerende kaders na (i.e. zowel Nederlandse als Europese regels) bij het verwerken van persoonsgegevens en heeft daartoe haar verantwoordelijkheid over de persoonsgegevens en die van andere duidelijk in kaart gebracht. Aveleijn monitort daarenboven ook de in de sector geldende gedragscodes en past deze toe.
10. We kunnen aantonen dat alle beleidsdoelstellingen worden nageleefd, conform de wettelijke bepalingen. Deze verantwoordingsplicht wordt bewaakt door interne toezicht en controle en is uitvoerbaar volgens de wettelijk geldende principes.

8 Overzicht verwerkingen

Voor elke applicatie die in gebruik is binnen Aveleijn wordt bijgehouden welke persoonsgegevens worden verwerkt. In het document staat tevens de bewaartermijn en de groepen die toegang hebben tot de data. De verwerkingen worden geregistreerd in het applicatielandschap. De architectuur richtlijnen van VGN worden gebruikt om processen te beschrijven. Binnen de processen worden applicaties gebruikt. Verwerkingen maken gebruik van deze applicaties en worden beschreven in het verwerkingsregister. Hierin worden de volgende zaken geregistreerd:

- de naam en contactgegevens van de verantwoordelijke;
- een beschrijving van de categorieën van betrokkenen en persoonsgegevens;
- een omschrijving van de verwerkingsdoeleinden;
- de wettelijke grondslag voor de gegevensverwerking;
- de categorieën van ontvangers van de persoonsgegevens;
- de bewaartermijnen (indien mogelijk);
- een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen (voor zover mogelijk);
- en een vermelding van verstrekking van persoonsgegevens aan een land buiten de Europese Unie of aan een internationale organisatie (indien van toepassing).

8.1 Bewaartermijnen

Documenten worden bewaard volgens een van tevoren bepaalde bewaartermijn. Voor verschillende soorten data is de bewaartermijn bepaald. Dit is beschreven in het document overzicht bewaartermijnen. Voor een deel van de data is dit wettelijk bepaald, de rest bepaalt Aveleijn zelf. De FG kan aangeven hoe de bewaartermijn van de data is bepaald.

8.2 Activiteiten als gevolg van de implementatie van het informatiebeveiligingsbeleid

Om te voldoen aan de AVG moeten de onderstaande gegevens voor alle applicaties in het verwerkingsregister worden opgenomen. Het verwerkingsregister is in ontwikkeling en een link naar dit register wordt in een volgende revisie meegenomen.

Hierin staan de volgende gegevens

- de naam en contactgegevens van de (interne) verantwoordelijke;
- een beschrijving van de categorieën van betrokkenen en persoonsgegevens;
- een omschrijving van de verwerkingsdoeleinden;
- de wettelijke grondslag voor de gegevensverwerking; (in lijst alleen ja/nee, en in kwaliteitshandboek de detaillering.
- de categorieën van ontvangers van de persoonsgegevens; (wie en via welke koppelingen)
- de bewaartermijnen
- een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen gekoppeld aan de opgestelde verwerkersovereenkomst.
- en een vermelding van verstrekking van persoonsgegevens aan een land buiten de Europese Unie of aan een internationale organisatie (indien van toepassing).

9 Gekoppelde processen

9.1 Datalek proces

Het datalek proces is beschreven in het proces meldplicht datalekken. Dit is via de kwaliteitshandboek via intranet beschikbaar.

9.2 Inzage, correctie en verwijderrecht

Deze rechten worden in een aparte procesbeschrijving nader beschreven per afdeling

9.3 Informatieverstrekking aan de betrokkene

Als bij de betrokkene de persoonsgegevens worden verkregen, deelt de verantwoordelijke vóór het moment van verkrijging de betrokkene het volgende 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.

9.4 Recht op inzage en afschrift van opgenomen persoonsgegevens

- De betrokkene heeft het recht kennis te nemen van de op zijn persoon betrekking hebbende verwerkte gegevens.
- De gevraagde inzage en/of het gevraagde afschrift zal zo spoedig mogelijk, doch uiterlijk binnen vier weken, plaatsvinden ofwel worden verstrekt.
- Een mogelijke beperkingsgrond voor inzage en afschrift kunnen gewichtige belangen van anderen dan de betrokkene/verzoeker zijn. Hieronder wordt ook de verantwoordelijke begrepen.
- Voor de verstrekking van een afschrift wordt geen vergoeding in rekening worden gebracht voor de gemaakte kosten

9.5 Recht op verbetering, aanvulling, verwijdering of afscherming

De betrokkene kan de verantwoordelijke verzoeken om de hem betreffende persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen als deze:

- feitelijk onjuist zijn;
- voor het doel of de doeleinden van de verwerking onvolledig zijn;
- niet ter zake dienend zijn; of
- anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen. Onder 'verwijdering' wordt ook vernietiging verstaan.

De verantwoordelijke vraagt de verzoeker binnen 4 weken na ontvangst van het verzoek schriftelijk of aan bovenstaande eisen voldaan kan worden.

De verantwoordelijke zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

Hij stelt derden (sub verwerkers) aan wie de gegevens daaraan voorafgaand zijn verstrekt, zo spoedig mogelijk hiervan in kennis, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost. De verantwoordelijke doet aan de verzoeker opgave van degenen aan wie hij die mededeling heeft gedaan.

Voor zorggegevens geldt dat in geval van een verzoek binnen 3 maanden wordt afgehandeld.



9.6 Toegangscontrole en bezoekersregistratie

Wordt beschreven in een volgende revisie.

9.7 Social Media beleid

Voor alle medewerkers is een social mediabeleid beschreven. Hierin wordt uitgelegd hoe medewerkers van Aveleijn omgaan met social media. Er worden richtlijnen beschreven over het gebruik van social media.

9.8 Camera gebruik

Wordt beschreven in een volgende revisie.