Privacybeleid van de stichting christelijke zorgorganisatie Norschoten

Maart 2021

Inhoud

1. Inleiding

1.1 Waarom een privacybeleid?

De Algemene Verordening Gegevensbescherming (hierna: AVG) stelt het opstellen van privacybeleid verplicht[1], als onderdeel van de verantwoordingsplicht voor zorgorganisaties zoals Norschoten die bijzondere persoonsgegevens (gegevens met betrekking tot de gezondheid) verwerken. Naast dit privacybeleid heeft Norschoten ook het informatiebeveiligingsbeleid opgesteld (in 2020 geschreven naar aanleiding van de NEN7510).

Het privacybeleid van Norschoten is gebaseerd op de privacyregels neergelegd in de AVG en sectorspecifieke wetten zoals de Wet op de geneeskundige behandelingsovereenkomst (Burgerlijk Wetboek boek 7, titel 7, Afd.5 / (Wgbo) en de Wet zorg en dwang (Wzd) etc. Zie bijlage 1 voor de inhoudelijke uitwerking van deze wetten bij dit beleid.

Het privacybeleid van Norschoten betreft een weergave op grote lijnen: voor bijzondere uitwerking van privacyonderwerpen wordt in de tekst verwezen naar andere documenten die Norschoten op dit vlak heeft opgesteld.

Het privacybeleid is van toepassing binnen Norschoten en heeft betrekking op de verwerkingen van gegevens van cliënten en medewerkers en is van toepassing op zowel op papier als elektronische verwerking van gegevens.

1.2 Definities die worden gehanteerd in het privacybeleid

Autoriteit Persoonsgegevens (AP): de toezichthoudende autoriteit, de onafhankelijke instantie die erover waakt dat persoonsgegevens zorgvuldig en veilig worden verwerkt en zo nodig sancties kan opleggen als dat niet gebeurt.

Bestand: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn.

Betrokkene: degene op wie een persoonsgegeven betrekking heeft, meestal de cliënt, of zijn (wettelijk) vertegenwoordiger of de medewerker/stagiaire/vrijwilliger/uitzendkracht.

Bijzondere categorieën persoonsgegevens: persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en 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.

Derde: elke persoon of instantie die geen betrokkene, verwerkingsverantwoordelijke, verwerker, of een persoon is die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is persoonsgegevens te verwerken.

Functionaris voor gegevensbescherming (FG): functionaris die door Norschoten is aangesteld voor het informeren en adviseren over en het toezicht houden op de toepassing en naleving van de AVG en andere gegevensbeschermingsbepalingen.

Gezondheidsgegevens: gegevens over de lichamelijke of geestelijke gezondheid van een persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt

1 Zie artikel 24 lid 2 AVG

gegeven;

Inbreuk in verband met persoonsgegevens: 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. Onder een 'datalek' valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkenen kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Toestemming van de betrokkene: door betrokkene, op goede informatie berustende, specifieke, in vrijheid en ondubbelzinnig gegeven toestemming waarbij betrokkene hem betreffende verwerking van persoonsgegevens aanvaardt. Dat kan door middel van een schriftelijke of mondelinge verklaring of een ondubbelzinnige actieve handeling (zoals het elektronisch aanvinken van een hokje).

Verwerker: degene die in opdracht van en voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt (bijvoorbeeld een externe hostingsfirma, saas-leverancier, kwaliteitsauditor of een extern salarisadministratiekantoor).

Verwerking van persoonsgegevens: alle 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 in een andere vorm beschikbaar stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke: degene die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; dit is de Raad van Bestuur van Norschoten (hierna Norschoten).

2. Verwerking van persoonsgegevens in overeenstemming met de AVG

2.1 Beginselen inzake verwerking persoonsgegevens[2]

Norschoten is verantwoordelijk voor de naleving van onderstaande beginselen bij de verwerking van persoonsgegevens en moet daarnaast ook de naleving van deze beginselen kunnen aantonen ("verantwoordingsplicht").[3]

[2] Let op: in de AVG wordt de rechtmatig van de verwerking van persoonsgegevens geregeld in artikel 6. Dat artikel staat echter na het artikel over de beginselen inzake de verwerking (zoals doelbinding, juistheid, etc.). Maar, als er geen grondslag is voor rechtmatige gegevensverwerking, mag er helemaal niet verwerkt worden en komt men dus niet toe aan de beginselen die moeten worden nageleefd bij de verwerking van persoonsgegevens.

[3] De beginselen inzake verwerking de verwerking van persoonsgegevens en de verantwoordingsplicht volgen uit artikel 5 AVG.

Binnen Norschoten mogen persoonsgegevens alleen worden verwerkt:

- op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is;
- voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt;
- de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt[4] niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd ("doelbinding");
- voor zover zij toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking" ook wel "dataminimalisatie" genaamd);
- indien de persoonsgegevens juist zijn en zo nodig worden geactualiseerd. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren ("juistheid");
- en bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt[5] mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen ("opslagbeperking");
- door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ("integriteit en vertrouwelijkheid").

2.2. Rechtmatigheid van de verwerking[6]

De verwerking is alleen rechtmatig indien en voor zover aan ten minste één van de onderstaande voorwaarden (zijnde de grondslagen voor de verwerking) is voldaan:

- de betrokkene heeft toestemming[7] gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden; Norschoten moet de toestemming kunnen aantonen en betrokkenen heeft het recht de toestemming te allen tijde in te trekken;
- de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, bijvoorbeeld de zorgverleningsovereenkomst met de cliënt of arbeidsovereenkomst met de medewerker;
- de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen, bijvoorbeeld de dossierplicht op grond van de Wgbo of gegevensverstrekking bij gedwongen opname en onvrijwillige zorg op grond van de Wet zorg en dwang;
- de gegevensverwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of een ander natuurlijk persoon[8];
- de gegevensverwerking noodzakelijk is voor de goede vervulling van een taak van algemeen belang, dat elders in een wet is vastgelegd met eventuele nadere bepalingen;
- de gegevensverwerking noodzakelijk is voor de behartiging van de gerechtvaardigde

[4] Overeenkomstig artikel 89, eerste lid, AVG.
[5] Overeenkomstig artikel 89, eerste lid, AVG.
[6] Artikel 6 AVG.
[7] Voor de voorwaarden die aan de toestemming zijn verbonden, zie definities.
[8] De AVG geeft in overweging (46) aan dat de verwerking van persoonsgegevens ook als rechtmatig wordt beschouwd indien zij noodzakelijk is voor de bescherming dat voor het leven van de betrokkene of dat van een ander persoon essentieel is. Deze grond voor verwerking is slechts toegestaan als de verwerking kennelijk niet op een andere rechtsgrond kan worden gebaseerd.

belangen[9] van de verwerkingsverantwoordelijke of van een derde én de belangen, grondrechten of fundamentele vrijheden van degene van wie de gegevens worden verwerkt niet prevaleren.

2.3 Voorwaarden voor het verwerken van bijzondere persoonsgegevens

Het is in de AVG verboden bijzondere categorieën persoonsgegevens zoals gezondheidsgegevens te verwerken, tenzij voldaan wordt aan één van de onderstaande voorwaarden[10]:

- de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden;
- de verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere persoon, indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven (zoals acute zorg);
- de verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, mits de verwerking uitsluitend betrekking heeft op de (voormalige) leden of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt;
- de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt; of
- de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid.

Let op: naast de opheffing van het verbod om bijzondere gezondheidsgegevens te verwerken zoals hierboven genoemd, moet dus ook nog een verwerkingsgrondslag aanwezig zijn om dergelijke gegevens te verwerken (zie hiervoor 2.2).

2.4 Gegevensverwerking door een verwerker

- Norschoten kan de verwerking van persoonsgegevens extern uitbesteden aan een zogeheten verwerker. De verplichtingen uit de AVG worden vastgelegd in een verwerkersovereenkomst die de verwerker ten aanzien van Norschoten bindt en waarin het onderwerp, de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen en de rechten en verplichtingen van Norschoten worden omschreven[11]. Het uitgangspunt is dat Norschoten het model verwerkersovereenkomst hanteert

[9] In overweging (47) en (49) AVG: een gerechtvaardigd belang kan aanwezig zijn wanneer sprake is van een relevante en passende verhouding tussen de betrokkene en de verwerkingsverantwoordelijke, in situaties waarin de betrokkene een klant is of in dienst is van de verwerkingsverantwoordelijke. In elk geval is een zorgvuldige beoordeling geboden om te bepalen of er sprake is van een gerechtvaardigd belang. De belangen en de grondrechten van de betrokkene kunnen met name zwaarder wegen wanneer persoonsgegevens worden verwerkt in omstandigheden waarin de betrokkenen redelijkerwijs geen verdere verwerking verwachten. De verwerking van persoonsgegevens voor zover die strikt noodzakelijk en evenredig is met het oog op netwerk- en informatiebeveiliging vormt een gerechtvaardigd belang van de verwerkingsverantwoordelijke in kwestie.

[10] Artikel 9 AVG en Artikel 22 Uitvoeringswet AVG . Verwerkingsverbod bijzondere categorieën persoonsgegevens en algemene uitzonderingen uit verordening. Bijzondere persoonsgegevens zijn gegevens die bestaan uit gegevens over 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 .

[11] Artikel 28 AVG.

die ActiZ in BOZ verband heeft opgesteld.

- De verwerker en een ieder die onder het gezag van Norschoten of van de verwerker handelt en toegang heeft tot persoonsgegevens, verwerkt deze uitsluitend in opdracht van Norschoten, tenzij hij door wet- of regelgeving tot verwerking gehouden is.[12]

2.5 Aansprakelijkheid verwerkingsverantwoordelijke en/of verwerker

1. Norschoten (de verwerkingsverantwoordelijke) is verantwoordelijk en aansprakelijk voor schade die voortvloeit uit het toerekenbaar tekortschieten of niet voldoende naleven van de AVG, waaronder het wel/niet naleven van de beveiligingseisen.
2. De verwerker, waaraan Norschoten (een deel van) de gegevensverwerking heeft uitbesteed, kan daarnaast zelfstandig aansprakelijk zijn voor schade of een deel van de schade die voortvloeit uit zijn werkzaamheden. Hoe die aansprakelijkheid wordt verdeeld, wordt beoordeeld door de schadeverzekeraar of de rechter. Van belang is dat Norschoten daarom goede afspraken maakt met de verwerker en deze vastlegt in een verwerkersovereenkomst.

2.6 Wanneer mogen andere bijzondere gegevens worden verwerkt?

Andere bijzondere gegevens, bijvoorbeeld gegevens met betrekking tot ras of godsdienst mogen bij cliënten alleen als aanvulling op gezondheidsgegevens worden verwerkt als dat nodig is voor een goede behandeling of verzorging van de betrokkene en dus niet systematisch bij elke cliënt. Bijvoorbeeld voor de inschakeling van een tolk als dat voor de uitleg van de behandeling aan cliënt nodig is. Bij medewerkers mag Norschoten bijvoorbeeld alleen gegevens over hun ras in hun personeelsdossier opnemen als dat nodig is om medewerkers te kunnen identificeren (denk aan pasfoto waaruit het ras blijkt) of om een voorkeursbeleid (positieve discriminatie) toe te passen.

2.7 Geheimhoudingsplicht en verstrekking aan derden

1. Persoonsgegevens verkregen in de uitoefening van een beroep in de gezondheidszorg vallen onder de geheimhoudingsplicht van de hulpverlener. Deze geheimhoudingsplicht is o.a. vastgelegd in de Wgbo en de wet BIG en in verschillende beroepscodes.
2. Bij de verstrekking van gegevens aan derden wordt de wet nageleefd. Handreiking die hierin behulpzaam kan zijn is de wegwijzer beroepsgeheim in samenwerkingsverbanden.

2.8 Wanneer mogen gegevens worden verstrekt voor wetenschappelijk onderzoek en statistiek?

De gegevensverwerking met het oog op archivering in het algemeen belang, wetenschappelijk onderzoek of statistische doeleinden is onderworpen aan passende waarborgen in overeenstemming met de AVG voor de rechten en vrijheden van de betrokkene. Deze maatregelen kunnen pseudonimisering omvatten, mits aldus die doeleinden in kwestie kunnen worden verwezenlijkt. Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt.[13]
Verder kan er in wetgeving worden afgeweken indien dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken.

Zo geeft de Wgbo[14] onderstaande afwijkende bepalingen voor wetenschappelijk onderzoek op het gebied van de gezondheidszorg. Het uitgangspunt is dat voor het verstrekken van niet geanonimiseerde[15] gegevens toestemming van de cliënt is vereist. In afwijking van dit uitgangspunt kan

[12] Artikel 29 AVG.
[13] Artikel 89 AVG.
[14] Artikel 7:457 en 7:458 BW (Wgbo).
[15] Pseudonimisering is een beveiligingsmaatregel (versleuteling of apart opslaan van identificerende gegevens los van de inhoudelijke) die direct herleiden tot een natuurlijke persoon onmogelijk maakt, maar indirecte herleiding (bijvoorbeeld door koppeling aan andere reeds bekende gegevens) blijft mogelijk. Daarom blijven gepseudonimiseerde gegevens persoonsgegevens en blijven de AVG-bepalingen en die uit de sectorspecifieke wetten over privacy van

ook zonder toestemming van de cliënt ten behoeve van statistiek of wetenschappelijk onderzoek op het gebied van de volksgezondheid aan een ander desgevraagd inlichtingen over de cliënt of inzage in de bescheiden worden verstrekt indien:

1. het vragen van toestemming in redelijkheid niet mogelijk is[16] en bij de uitvoering van het onderzoek zodanige waarborgen gelden, dat de persoonlijke levenssfeer van de cliënt niet onevenredig wordt geschaad, of
2. het vragen van toestemming, gelet op de aard en het doel van het onderzoek, in redelijkheid niet kan worden verlangd en de hulpverlener ervoor zorgt dat gegevens in zodanige vorm worden verstrekt dat herleiding tot individuele natuurlijke personen redelijkerwijs wordt voorkomen.

Verder moet:

a) het onderzoek een algemeen belang dienen;
b) aangetoond zijn dat het onderzoek niet zonder de gegevens kan worden uitgevoerd; en
c) de betrokken cliënt tegen een verstrekking niet uitdrukkelijk bezwaar heeft gemaakt.

Bovenstaande voorwaarden werken cumulatief dus verstrekking is pas mogelijk indien aan alle voorwaarden is voldaan.

Norschoten (de verwerkingsverantwoordelijke) en de onderzoeker maken schriftelijke afspraken over de maatregelen die de onderzoeker neemt om de privacy van betrokkenen te beschermen.

2.9 Bewaren van persoonsgegevens

Norschoten dient de (papieren en digitale) persoonsgegevens op een veilige wijze te bewaren, die in overeenstemming is met de geldende wet- en regelgeving. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is om de doelen te bereiken waarvoor de gegevens worden verwerkt, tenzij de gegevens worden geanonimiseerd of indien het noodzakelijk is voor de uitoefening van het recht op vrijheid van meningsuiting en van informatie, voor de nakoming van een wettelijke verplichting, voor de uitvoering van een taak in het algemeen belang of in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend, om redenen van algemeen belang op het vlak van volksgezondheid, met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden of voor de vaststelling, uitoefening of onderbouwing van een rechtsvordering.[17]

Norschoten heeft vastgesteld hoelang de vastgelegde/geregistreerde persoonsgegevens bewaard blijven in overeenstemming met de geldende wet- en regelgeving. Indien nog geen specifieke termijn kan worden genoemd dan gelden de algemene criteria voor het vaststellen van de bewaartermijn. Zie voor dit overzicht van geldende bewaartermijnen de notitie Bewaren en vernietigen van documenten op het Kwaliteitshandboek.

3 Rechten van de betrokkenen: opgenomen in de privacyverklaringen

De AVG geeft aan wat de rechten van de betrokkene zijn zoals recht op inzage, informatie, vernietiging van de persoonsgegevens (artikel 12-14 AVG). Persoonsgegevens mogen alleen van de betrokkene worden verwerkt wanneer voor hem of haar, onder andere, transparant is wat er met diens

toepassing. Zie ook overweging (29) AVG.

[16] Bijvoorbeeld als het gaat om een historisch onderzoek naar jaren geleden verzamelde gegevens over personen van wie de adressen niet meer te achterhalen zijn. *Kamerstukken II*, 21561, 20, p. 3.

[17] Artikel 17, derde lid, AVG (overweging 65).

persoonsgegevens gebeurt (transparantiebeginsel). Dit betekent dat Norschoten verplicht is informatie te verschaffen aan betrokkenen over de gegevensverwerkingen. Norschoten heeft voor zowel cliënten als voor medewerkers hiervoor een privacyverklaring opgesteld. Deze beide verklaringen zijn op het Kwaliteitshandboek terug te vinden en de privacyverklaring voor cliënten staat daarnaast ook nog op de website van Norschoten.

4 Veilige verwerking van persoonsgegevens

4.1 Verantwoordelijkheid van Norschoten zijnde de verwerkingsverantwoordelijke[18]

1. Norschoten treft passende technische en organisatorische maatregelen (zie lid 2) om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.
2. Norschoten is bezig met een certificeringstraject ten aanzien van NEN 7510 en wil, door uitgebreider stil te staan bij een aantal specifieke maatregelen uit deze norm, ook meteen voldoen aan de NEN 7512 en NEN 7513. Norschoten is voornemens om in de zomer van 2021 gereed te zijn voor de interne audit als voorbereiding op de certificeringsaanvraag. Norschoten kan daardoor aantonen dat zij voldoet aan de algemeen geldende informatiebeveiligingseisen en dat passende technische en organisatorische maatregelen zijn getroffen om deze te waarborgen.
3. Voor de verstrekking van bijzondere persoonsgegevens en andere gevoelige informatie via e-mail wordt binnen Norschoten gebruik gemaakt van ZorgMail secure email.
4. De standaardinstellingen en vragenlijsten zijn altijd zo ingericht dat er toestemming wordt gevraagd (opt-in) in plaats van vooraf al ja ingevuld op een formulier (opt-out).
5. Norschoten hanteert een rol/locatie gebaseerde autorisatieprocedure voor verwerking van persoonsgegevens (van cliënten). Dat bepaald welke gegevens door wie/welke (groepen) medewerkers verwerkt kunnen worden en welke bevoegdheden zij hebben ten aanzien van welke gegevens (inzage, toevoegen, wijzigen, verwijderen).

4.2 Gezamenlijke verwerkingsverantwoordelijken[19]

1. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze AVG vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene en hun respectieve verplichtingen om de verplichte informatie te verstrekken, door middel van een onderlinge regeling. In de regeling kan een contactpunt voor betrokkenen worden aangewezen. Norschoten heeft hiervoor een standaardovereenkomst opgesteld.
2. Ongeacht een dergelijke regeling kan een betrokkene zijn rechten uit de AVG met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen.

4.3 Register van verwerkingen[20]

Norschoten dient een register bij te houden van de verwerkingsactiviteiten die onder haar verantwoordelijkheid plaatsvinden. Dat register bevat in ieder geval de volgende gegevens:

a) de naam en de contactgegevens van de zorgaanbieder en eventuele gezamenlijke verwerkingsverantwoordelijken, en van de functionaris voor gegevensbescherming;
b) de verwerkingsdoeleinden;
c) een beschrijving van de categorieën van betrokkenen en van de categorieën van

[18] Artikel 24 AVG.
[19] Artikel 26 AVG.
[20] Artikel 30 AVG.

persoonsgegevens;

d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
e) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, van de AVG bedoelde doorgiften, de documenten inzake de passende waarborgen;
f) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
g) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

4.4 Melding van datalekken aan de Autoriteit Persoonsgegevens en het datalekkenregister[21]

1. Indien een inbreuk in verband met persoonsgegevens (ook wel datalek genoemd) heeft plaatsgevonden, meldt Norschoten dit zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat Norschoten er kennis van heeft genomen, aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de Autoriteit Persoonsgegevens niet binnen 72 uur plaatsvindt, wordt de vertraging toegelicht (gemotiveerd).
2. De verwerker informeert Norschoten conform de verwerkersovereenkomst zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.
3. Norschoten heeft een protocol " Meldplicht datalekken en stappenplan" opgesteld waarin wordt aangegeven welke stappen een medewerker moet nemen bij een vermeende datalek of ander privacy incident. Dit protocol staat op het Kwaliteitshandboek van Norschoten.
4. Norschoten houdt alle inbreuken in verband met persoonsgegevens bij in een overzicht, met inbegrip van de feiten omtrent die inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen. Dit overzicht stelt de Autoriteit Persoonsgegevens, de accountant en auditoren in staat de naleving van dit artikel te controleren.

4.5 Datalek melden aan de betrokkene[22]

1. Wanneer de datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt Norschoten de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.
2. De mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:
   a) Norschoten heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
   b) Norschoten heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
   c) de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.
3. Indien Norschoten de datalek nog niet aan de betrokkene heeft gemeld, kan de Autoriteit Persoonsgegevens, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, Norschoten daartoe verplichten of besluiten dat aan een van de in lid 2 van dit artikel, bedoelde voorwaarden is voldaan.

[21] Artikel 33 AVG.
[22] Artikel 34 AVG.

4.6 Data Protection Impact Assessment (DPIA)

1. Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van cliënten of medewerkers voert Norschoten vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.[23]
2. Voor het uitvoeren van een DPIA moet altijd het advies van de FG worden ingewonnen.
3. Een DPIA als bedoeld in het eerste lid is met name vereist in de volgende gevallen:
    a) er sprake is van een grootschalige verwerking van bijzondere categorieën van persoonsgegevens, zoals gezondheidsgegevens;
    b) er sprake is van stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten (denk aan cameratoezicht).
4. Wanneer uit een DPIA blijkt dat de verwerking een hoog risico zou opleveren indien Norschoten geen maatregelen neemt om het risico te beperken, raadpleegt Norschoten voorafgaand aan de verwerking de Autoriteit Persoonsgegevens.
5. Norschoten heeft een model waarmee een DPIA kan worden uitgevoerd en waarin de opgesomde eisen in artikel 3.4.7 en in de AVG zijn meegenomen.

5. Functionaris voor gegevensbescherming (FG)

5.1 Aanwijzing en positie van een functionaris voor gegevensbescherming[24]

1. Norschoten heeft een functionaris voor gegevensbescherming (FG) aangewezen en deze is geregistreerd bij de Autoriteit Persoonsgegevens.
2. Norschoten heeft gekozen voor een FG die tevens medewerker is.
3. Norschoten zorgt ervoor dat de FG geen instructies ontvangt met betrekking tot de uitvoering van die taken; de FG werkt zelfstandig en onafhankelijk. De FG wordt door Norschoten niet ontslagen of gestraft voor de uitvoering van zijn taken en ondervindt geen nadeel van de uitoefening van zijn taak. De FG brengt rechtstreeks verslag uit aan de Raad van Bestuur.
4. De FG is bereikbaar onder fg@norschoten.nl

5.2 Taken van de FG

De FG vervult ten minste de volgende taken:

a) het informeren en adviseren over de verplichtingen van de medewerkers ten aanzien van de privacywetgeving (de AVG en andere sectorspecifieke wet- en regelgeving);
b) toezien op naleving van deze wetgeving en van het beleid van Norschoten met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
c) desgevraagd advies verstrekken met betrekking tot de DPIA en toezien op de uitvoering daarvan;
d) toezien dat er verweerkersovereenkomsten worden afgesloten indien nodig;
e) toezien dat het register van verwerkingen actueel is;
f) met de Autoriteit Persoonsgegevens samenwerken en als contactpunt optreden.

[23] De Autoriteit Persoonsgegevens heeft een lijst opgesteld van het soort verwerkingen waarvoor DPIA verplicht is. Deze lijst is verwerkt in het model dat Norschoten hanteert.
[24] Artikel 37 AVG.

5.3 Bij een klacht

Bij een klacht over de naleving van het privacybeleid kan de betrokkene zich wenden tot de FG (fg@norschoten.nl) :
Voor andere klachten raadpleegt de betrokkene de klachtenregeling van de Norschoten die op de website van Norschoten te raadplegen is.

Het meest recente privacybeleid staat op het Kwaliteitshandboek van Norschoten.

Bijlage 1. Relatie AVG met andere wetten

Algemene Verordening Gegevensbescherming (AVG)

De AVG is een Europese verordening die regels stelt voor gegevensverwerkingen en heeft als doel persoonsgegevens te beschermen. Uit de AVG volgt dat het verboden is om bijzondere categorieën persoonsgegevens, zoals gezondheidsgegevens, te verwerken tenzij aan bijzondere (strengere) regels uit de AVG wordt voldaan. Deze Europese verordening laat op een aantal plaatsen ruimte aan de nationale wetgever om eigen regels in nationale wetgeving verder te regelen zoals de uitwerking van bijzondere persoonsgegeven ("gevoelige gegevens"). Deels wordt dit geregeld in een (Nederlandse) uitvoeringswet (UAVG). De AVG biedt de lidstaten ook ruimte om eigen regels voor de toepassing vast te stellen in sectorspecifieke wetten zoals met betrekking tot geneeskundige gezondheidszorg (Wgbo en Wzd) en met betrekking tot het sociaal domein (Wmo 2015).

Voor de gezondheidzorg belangrijkste wetten wordt hieronder aangegeven hoe zij zich verhouden tot de AVG en tot elkaar.

Relatie met Wgbo

De regels uit de Wet op de geneeskundige behandelingsovereenkomst (Wgbo) blijven bestaan naast de AVG.
Net als nu is Norschoten onder de AVG dus gebonden aan zowel de regels over het medisch beroepsgeheim uit de Wgbo als aan de regels van de AVG. Als zorgaanbieder mag je bijvoorbeeld alléén gegevens aan een derde verstrekken als dat mag op grond van de AVG én als je een grond hebt om het medisch beroepsgeheim te doorbreken.

Relatie met Wet zorg en dwang

Ook de Wzd is een sectorspecifieke wet die de toepassing regelt naast de AVG met betrekking tot de verwerking van gezondheidsgegevens bij onvrijwillige zorgverlening. Dit betekent dat specifieke privacybepalingen in de Wzd naast de AVG gelden voorrang krijgen (zijnde een lex specialis) ten opzichte van bepalingen die volgen uit de Wgbo. Bijvoorbeeld wat betreft de bijzondere bepalingen op de dossierplicht van de hulpverlener.

Relatie met de Zvw

De Zvw geeft ook bepalingen over privacy van de verzekerde/cliënt die bijvoorbeeld geriatrische revalidatie krijgt. Ook deze bepalingen gelden naast de bepalingen van de AVG. Een voorbeeld is het verplicht gebruik maken van het BSN door de zorgverzekeraar en gegevensverstrekking aan derden maar ook de bevoegdheid van de zorgverzekeraar tot controle of de gedeclareerde zorg ook werkelijk

door de zorgaanbieder geleverd is.
Dit is echter geen vrijbrief voor ongelimiteerde gegevensverzoeken en/of -verstrekking; de zorgverzekeraar ontvangt slechts gegevens die noodzakelijk zijn voor zijn controle, niet meer en neemt bij materiële controles eventueel genoegen met inzage in gegevens waarover alleen de zorgaanbieder beschikt. De zorgverzekeraar moet zich bovendien houden aan de controlestappen in de Regeling zorgverzekering wat betreft de formele en materiële controles.

Relatie met de Wlz

De Wlz geeft bepalingen over privacy van cliënten die behandeling (met opname) nodig hebben. Een voorbeeld is het verplicht gebruik van het BSN en gegevensverstrekking aan maar ook de controle of de gedeclareerde zorg ook daadwerkelijk is geleverd. De Wlz geeft tevens “Wgbo-achtige” bepalingen en stelt bijzondere eisen aan het opstellen en de inhoud van een zorgplan met de cliënt. De Wlz is een specifieke wet ten opzichte van de Wgbo. De AVG blijft daarentegen naast de Wlz gelden.

Relatie met Wmo 2015

De Wmo 2015 geeft bepalingen over privacy van de cliënt die een algemene- of maatwerkvoorziening krijgt, bijvoorbeeld begeleiding of dagbehandeling.