SET-up
TOOLKIT

Privacy compliance

Inleiding

Als zorgverlener verwerk je persoonsgegevens en moet je je houden aan de privacywetgeving en eisen vanuit overige zorgwetten. De belangrijkste privacywet is de Europese Algemene verordening gegevensbescherming (AVG). Deze wet bepaalt wat je allemaal mag doen met persoonsgegevens en hoe je deze gegevens moet beschermen.
Als zorgverlener ben je altijd vertrouwelijke persoonsgegevens aan het 'verwerken'. Denk aan het verzamelen, opslaan, wijzigen, aanvullen of doorsturen van gegevens. Zelfs als je gegevens anoniem maakt of verwijdert, ben je ze aan het verwerken (zij het met minder risico).
Gegevens zijn persoonsgegevens als ze gaan over personen die je kunt onderscheiden van andere personen. Dat noemen we een geïdentificeerde persoon. Je hebt een persoon bijvoorbeeld geïdentificeerd als je zijn voornaam en achternaam weet. Heb je iemand nog niet geïdentificeerd, maar kun je dat wel zonder al te veel moeite doen? Dan is die persoon alsnog 'identificeerbaar'. De persoon van wie je persoonsgegevens verwerkt heet de betrokkene.

Zie 1_Algemene AVG brochure ondernemers

Kern van de wettelijke eisen

Eigenlijk alle wetten en richtlijnen eisen van een 'verwerker' in de basis dat deze goed zicht heeft op de verzamelde data, de risico's heeft ingeschat en waar nodig maatregelen heeft getroffen, dit kan uitleggen en laten zien en tenslotte op verzoeken van betrokkenen kan reageren.

Om dit te realiseren zijn via de overheid, de www.avghelpdeskzorg.nl en koepelorganisaties diverse plannen en documenten beschikbaar.

Vanwege het specifieke karakter van de SET innovatieclusters heeft SET UP vanaf november 2019 in samenwerking met expertorganisatie Baker Tilly IT Advisory een kennisstroom hierover opgestart.
Er zijn twee webinars verzorgd en om de clusters een snelle start te kunnen laten maken:

- Presenteren we dit startdocument op het leerplatform Embrace.VitaValley.nl
- Publiceren we op het leerplatform Embrace.VitaValley.nl een starterskit met handige documenten
- Organiseren we een meet up sessie via zoom om vragen te beantwoorden en ervaringen te delen

Basis is dat je zelf inzicht krijgt en risico's inschat

Startpunt voor elke verwerking van gegevens (ook als je een nieuwe start vanuit een innovatietraject) is dat je je afvraagt wáárom je de verwerking doet, wat je daarvoor aan gegevens nodig hebt en welk risico daarmee betrokkenen (waar je de gegevens van verwerkt) lopen.

Vervolgens kan je dan bedenken welke maatregelen 'proportioneel', dat wil zeggen passend bij doel en risico, te treffen zijn. Daarbij geldt altijd dat er een bepaald restrisico overblijft, wat je kan communiceren richting alle stakeholders.

Omdat je op die manier samen werkt aan inzicht en vertrouwen, werkt privacy-compliance innovatie niet tegen maar helpt het juist om 'het goede gevoel' en vertrouwen te krijgen bij bestuur, management en gebruikers!

Stap 1 Waarom verwerk je? Het bepalen van de grondslag

Als eerste – en dat is meestal door de functionaris gegevensbescherming al wel gedaan – bepaal je waarom en onder welke grondslag je gegevens verwerkt.

Een groot deel van de verwerkingen (zoals van je personeel) is wettelijk toegestaan. Ook onder de WGBO ben je als zorgverlener verplicht om een dossier te voeren en onder de Wet BSN in de Zorg om het BSN te registreren en gebruiken bij gegevensuitwisseling.

Als je geen grondslag in een wet vind, dan kan de grondslag ook worden verkregen via
- een (zakelijke) overeenkomst met de betrokkene
- in situaties van leven of dood (vitaal belang)
- ondubbelzinnig verkregen toestemming van de betrokkene (wat ook weer ingetrokken mag worden)
Deze toestemming is een laatste redmiddel, het houdt veel werk in wat betreft registratie en procedures rondom intrekken e.d.

Wat een beter alternatief is als laatste vorm van grondslag:

- gerechtvaardigd belang vanuit het doel van de verwerking

Naast een geldige grondslag, is er namelijk een gerechtvaardigd doel nodig (artikel 6 lid 4 AVG). Gegevens mogen op basis van een grondslag verwerkt worden, maar dat mag alleen voor een concreet bepaald doel. Die doelen staan niet in de AVG genoemd, die moet je als zorgverlener zelf opstellen en moeten gerechtvaardigd zijn. De verwerking van de persoonsgegevens mag alleen plaatsvinden voor dat doel.

Doelbinding: op basis van een grondslag verwerk je voor een doel

Voorbeeld: onder wettelijke grondslag verzamel je BSN (Wet BSN in zorg) en NAW en verzekeringsgegevens (WGBO). Gerechtvaardigde doelen onder deze grondslag kunnen zijn:
- verlenen van zorg
- verminderen fysiek contact om verspreiding COVID-19 te voorkomen
- verbeteren kwaliteit van leven
- ondersteuning van mantelzorgers
- communicatie met cliënten ter voorkoming van sociaal isolement
- verbeteren van zorg / doelmatigheid van de zorg
- evaluatie van kwaliteit / effectiviteit van de zorg
- eventueel wetenschappelijk onderzoek

Tenslotte moet je grondslag en doelen in een privacyverklaring (privacystatement) opnemen. Zo kun je bijvoorbeeld op basis van het gerechtvaardigd belang persoonsgegevens verwerken voor direct marketingdoeleinden. Soms kan een grondslag ook samenvallen met een doel. Zo kun je op basis van de grondslag wettelijke verplichting persoonsgegevens verzamelen met als doel te voldoen aan de administratieve bewaarplicht.

Zie 2_SET-up Webinar Privacy Compliance 12 mei 2020 DEF

Stap 2 Werk uit welke gegevens je daarvoor nodig hebt

Als je uiteindelijk je set van doelen hebt bepaald, ga je in een data inventarisatie onderbouwen voor welke activiteit je welke gegevens nodig hebt. Daarmee krijg je inzicht en kan je goed beslissen wat de minimaal benodigde dataset is (want je mag niet meer verwerken dan nodig voor je doel).

2A Welke activiteiten en doelen PROCES SCHEMA

Werk stappen in het zorgproces uit en bepaal per stap de doelbinding. Wees zo concreet mogelijk. Het doel: 'ik probeer mensen goede zorg te verlenen' is te algemeen. Een voorbeeld:
- doel: ondersteunen bij dagelijkse activiteiten
- stappen: het inlichten van de mantelzorger, het plannen van een afspraak, het begeleiden bij dagelijkse boodschappen, verslaglegging

2B Wat zijn de noodzakelijke gegevens per doel DATA

Bepaal vervolgens welke gegevens nodig zijn per stap en waarom die gegevens nodig zijn.
Stel vast bij welke bron je de gegevens zelf hebt of kan opvragen. Dit kan zijn de zorgconsument zelf, maar ook andere partijen als mantelzorg, ketenpartner, verzekeraar.
- Welke taak en rol heeft die organisatie en waarom stel je die vraag aan hen?

Let op dataminimalisatie: niet meer data dan nodig voor deze stap.

3 Vul een Privacy Impact Assessment in

De resultaten van bovenstaande analyses verwerk je vervolgens in een DPIA = Data Protection Impact Assessment (of ook wel Gegevensbeschermingseffect beoordeling genoemd).
Een DPIA dien je als organisatie uit te voeren voor je vaste verwerkingen (zoals je elektronisch systeem en je personeelssysteem) maar het is ook verplicht als je nieuwe processen / technieken introduceert.

Het doel van een DPIA is instrumenteler dan bij de data inventarisatie. Een DPIA is in feite een uitgebreide checklist waarmee je gestructureerd de karakteristieken van de gegevensverwerking en de gegevens naloopt om daarmee de hoogte van de risico's voor privacy voor betrokkenen in te schatten. Let wel: het is een risicoanalyse instrument en geen naleving instrument/checklist! Op basis hiervan kan je onderbouwd als organisatie aangeven waar de hoogste risico's worden gelopen en waar je dus ook het accent legt bij het treffen van maatregelen.

Zie 3_EU Richtlijnen PIA
4_Format PIA NOREA
5_PIA Uitleg NOREA
6_Rijksmodel PIA

4 Tref passende maatregelen uit

Met de risico analyse en het inzicht in waar welke gegevens het grootste risico lopen, kan je gericht maatregelen treffen. Natuurlijk heb je al veel maatregelen getroffen in je organisatie (zoals firewalls, virusprotectie, wachtwoorden en dergelijke), maar je zult zien dat je voor een innovatie vaak op een aantal gebieden extra maatregelen moet treffen.

Er bestaan diverse baselines/checklists voor maatregelen waarvan verwacht wordt dat je dit treft. Een heel bekende is de NEN 7510. Maar ook heeft de IGJ een toetsingskader 'Inzet van e-health door zorgaanbieders' gelanceerd. De beroepsorganisatie van IT auditors heeft een Privacy Control Framework uitgewerkt, waartegen je ook eenvoudig getoetst kan worden.

Het is belangrijk dat je op basis van een duidelijke kapstop (uit de hierboven genoemde kaders) uitwerkt welke maatregelen getroffen zouden moeten zijn en wat de actuele status is. Uit het verschil hiertussen volgt dan eenvoudig een actieplan, wat je ook weer op status kan bijhouden. Zo heb je altijd snel inzichtelijk voor cliënten en andere stakeholders en toezichthouders hoe goed je je best doet om risico's te beperken.

> In de privacywetgeving is het belangrijk dat je voor de hoogte van je aansprakelijkheid altijd goed kan laten zien wat voor maatregelen je hebt getroffen.

Zie 7_IGJ Toetskader eHealth
8_IGJ Toetskader compact
9_NOREA Privacy Control Framework

5 Controleer, evalueer en pas aan

Het is onder de wetgeving ook verplicht dat je vervolgens een controlesysteem hebt draaien waarin je ook actief in gaten houdt dat maatregelen daadwerkelijk doen wat ze moeten doen. In de NEN 7510 terminologie heet dit het Information Security Management Systeem (ISMS).
Als je interne kwaliteitsmedewerkers / auditoren hebt is het goed hen ook periodiek checks te laten doen op bijvoorbeeld clean desk, gebruik van wachtwoorden, loggingen van systemen (wie heeft welk dossier bekeken) etc. Dit levert een tijdige signaal en reactie wanneer zaken net iets anders lopen.

Tenslotte niet vergeten !

Je richt privacy-compliance in voor je klant, informeer hen dus ook altijd over je verwerkingen, je doelen en de intentie om passende maatregelen te treffen. Dit moet altijd via het formele kanaal (privacy-statement en procedures op site), maar vergeet ook niet het informele kanaal en de manier waarop je medewerkers op de hoogte zijn van risico's en dit ook uitdragen.

En laat jezelf periodiek challengen op je aanpak: laat een onafhankelijke blik eens een check doen, laat een review of audit uitvoeren en leer hiervan.

Over de auteur:

Wilco Brouwers is senior manager bij IT Advisory van Baker Tilly. Hij is ruim twintig jaar adviseur en IT-auditor. Hij heeft veel audit- en advieswerkzaamheden uitgevoerd bij zorgorganisaties, onder andere op het gebied van strategievorming, informatiebeveiliging en beheersing.
Wilco heeft een ruime periode bij CZ Zorgverzekeringen als IT audit manager gewerkt en daar nauw samengewerkt met zorginkopers en innovatiemanagers op de ontwikkeling en kwaliteitsbewaking van systemen in de zorg.

Wilco participeert momenteel actief in diverse gremia die actief zijn op dit gebied, zoals de SETP UP expert pool en het OPEN programma (VIPP programma voor ontsluiting eerstelijns systemen). Hij is tevens lid van de NOREA Kennisgroep Zorg & ICT en de NEN normcommissie 303 006 Informatievoorziening in de zorg. Baker Tilly is tevens partner van NEN in het programma 'Werken met NEN 7510'.