Privacy Impact Analyse

Voor het gebruik van LanCOS

Juni 2022

vereniging gehandicaptenzorg nederland

Inleiding

Op het moment van schrijven (juni 2022) werken in de verschillende crisisregio's de zorgaanbieders op heel verschillende manier samen. De informatie-uitwisseling vanuit zorgaanbieder heeft niet altijd hetzelfde beveiligingsniveau. Zorgverzekeraars Nederland (ZN) heeft daarom het initiatief genomen tot het laten ontwikkelen van een applicatie die de crisisondersteuningsteams (COT) op een veilige manier moet ondersteunen. Dat is LanCOS, ontwikkeld door ZorgMatch. Grofweg 50 zorgaanbieders hebben hiermee te maken. Zij hebben meerdere contracten en toelichtende documenten ontvangen.

De Algemene Verordening Gegevensbescherming stelt dat organisaties bij nieuwe verwerkingen van persoonsgegevens privacyrisico's behoren te inventariseren en maatregelen behoren te treffen. Dit is via een Data Protection Impact Assessment (DPIA) of Privacy Impact Assessment (PIA). Voor de ontwikkelfase hebben de Zorgverzekeraars Nederland het initiatief genomen voor een DPIA. Voor de gebruiksfase van LanCOS kunnen de zorgverzekeraars (Zorgkantoren) dit niet doen omdat zij in de gebruiksfase geen persoonsgegevens verwerken[1]. Om te voorkomen dat straks 50 zorgaanbieders een eigen DPIA gaan maken voor de gebruiksfase hebben drie zorgaanbieders het initiatief genomen tot het gezamenlijk opstellen van een DPIA en deze ter beschikking te stellen aan de overige zorgaanbieders die actief zijn in een Crisis- en OndersteuningsTeam. Omdat elk van de betrokken zorgaanbieders actief is in de VG-sector heeft de VGN als brancheorganisatie het opstellen van de voorliggende DPIA ondersteund. De drie zorgaanbieders die deze DPIA geschreven hebben zijn Cordaan, de Hartekamp Groep en 's Heeren Loo.

Ten tijde van het maken van deze DPIA was het nog niet mogelijk om alle beveiligingsmaatregelen in de software te beoordelen. Verder is tijdens het opstellen van de DPIA als uitgangspunt gehanteerd dat een zorgaanbieder die gebruik wil maken van deze DPIA alle benodigde contracten heeft ondertekend. Dit omdat er anders geen gebruiksrecht van de software is. Het is tenslotte de verantwoordelijkheid van elke individuele zorgaanbieder om te beoordelen of voorliggend document voldoende is om als DPIA in de eigen organisatie te kunnen dienen. Als dit document tenminste een eerste aanzet zou geven, dan is het doel van efficiency al bereikt.

Leeswijzer

Aan een DPIA zitten diverse aspecten. Per aspect beginnen we met een inleidende tekst, gevolgd door één of meer bevindingen met een privacyrisico. Per risico benoemen we maatregelen die een zorgaanbieder kan overwegen om het risico in te perken.

[1] Uitzondering hierop is als het Zorgkantoor fungeert als crisisregisseur.

Samenwerking binnen een COT

Landelijk bestaan verschillen hoe COT's samenwerken en uitvoering geven aan digitale uitwisseling, opslag van (persoons)gegevens. De nieuwe applicatie LanCOS biedt de mogelijkheid om processen op eenduidige vorm te geven dit volgens, in overeenstemming met afgesloten samenwerkings- en verwerkersovereenkomst.

Relevante documenten met (bijzondere) persoonsgegevens worden op een beveiligde (encryptie) manier geüpload en verwerkt binnen de applicaties LanCOS. Er bestaat echter een privacyrisico dat COT-leden naast het gebruik van LanCOS op andere, minder veilige, manieren (persoons)gegevens uitwisselen en in hun zakelijke dan wel privé omgeving opslaan.

Privacyrisico 1: gebruik van andere methoden voor gegevensuitwisseling
Het is mogelijk dat naast de applicatie LanCOS andere, onveilige toepassingen (zoals e-mail of chatapps) voor gegevensuitwisseling tussen COT-leden worden gebruikt.

Maatregel: Zorgaanbieder(s) maken gebruik van NTA 7516 gecertificeerde mail- en chattoepassingen (Zivver, SmartLockr, ZorgMail, e.d.).

Privacyrisico 2: gebruik van eigen ICT-omgeving door COT-leden voor gegevensverwerking
Het is mogelijk dat COT-leden naast LanCOS hun eigen ICT-omgeving (zoals Office 365) gebruiken voor het opslaan van persoonsgegevens van cliënten die bij een andere zorgaanbieder in zorg zijn. Dit is strijdig met **dataminimalisatie** art. 5, AVG.

Maatregel:
COT-deelnemende zorgaanbieders maken schriftelijke afspraken dat persoonsgegevens van een cliënt alleen verwerkt worden bij de zorgaanbieder waarbij cliënt in zorg is. En in de applicatie LanCOS waarvoor een gezamenlijke samenwerkings- en verwerkersovereenkomst is afgesloten.

Aard van de gegevens

De grondslag voor het verwerken van persoonsgegevens van Wlz-cliënten is 'toestemming' of in uitzonderlijke situaties 'vitaal belang'. De 'toestemming' wordt vastgelegd door de zorgaanbieder die de cliënt aanmeldt bij het COT.

In de applicatie LanCOS zijn contactgegeven van persoonsgegevens van gebruikers opgenomen maar primair betreft het bijzondere (medische) persoonsgegevens van cliënten:

- Getekend aanmeldformulier door cliënt (toestemmingsverklaring) met begeleidende (zorg- en medische) documenten
- Burgerservicenummer
- NAW- en bereikbaarheidsgegevens
- Zorgplannen in combinatie met (medische) persoonsgegevens
- Rapportages begeleidende zorgmedewerker(s) van een cliënt
- Medicatie, rapporten gedragsdeskundigen, e.d. psychologen en/ of psychiaters
- (Voortgangs)verslagen van COT-vergaderingen over een cliënt
- Gespreksverslagen die zijn gevoerd met een cliënt

Door de bijzondere persoonsgegevens zijn er strengere beveiligings- en privacymaatregelen vanuit de Algemene Verordening Gegevensbescherming van toepassing.

Privacyrisico 1: Ontbreken eigenaarschap vanuit COT's voor adequaat beheer van LanCOS
Het ontbreken van afspraken over het beheer van de applicatie LanCOS leidt tot 'vervuiling' van gebruikersaccounts en oneigenlijke toegang van COT-leden die geen betrokkenheid meer hebben.

Maatregel:
Een COT wijst een 'beheerder' aan voor de applicatie LanCOS. Deze beheerder verzorgt het toekennen, intrekken en het controleren van gebruiksaccounts en bijbehorende autorisaties van COT-leden. Desgewenst staat het COT's vrij dit formeel bij te houden via een Access Control List.

Privacyrisico 2: Persoonsgegevens worden overgenomen naar ICT-omgeving zorgaanbieder
Afhankelijk van het 'gebruiksgemak' en dus acceptatie bestaat het risico dat COT-leden bestanden downloaden vanuit de applicatie LanCOS. Of na het per e-mail rondsturen van documenten deze opslaan binnen hun eigen ICT-omgeving. Dit is strijdig met het uitgangspunt van **dataminimalisatie** vanuit de Algemene Verordening Gegevensbescherming.

Maatregel:
Samenwerkende zorgorganisaties en dus COT-leden hanteren een eenduidige wijze van digitale gegevensoverdracht en spraken af dat (bijzondere) persoonsgegevens van cliënten niet worden opgenomen in hun eigen ICT-omgeving[2].

[2] Dit geldt niet voor de COT-zorgaanbieder waarbij de client in zorg is. Deze zorgaanbieder fungeert als 'primaire' verwerkingsverantwoordelijke instelling na het einde van het COT-proces.

Betrokken partijen

Het COT bestaat uit een onafhankelijke crisisregisseur en experts van regionale zorgaanbieders. Het gebruik van de applicatie LanCOS is alleen mogelijk als een zorgaanbieder de samenwerkings- en verwerkingsovereenkomsten formeel heeft geaccepteerd. Door de ondertekening verklaren zorgaanbieders dat hun ICT-omgeving voldoet aan de NEN7510, NEN7512, NEN7513 en NTA7516 zoals gesteld in de Algemene verordening gegevensbescherming.

Privacyrisico 1: Beveiligingsmaatregelen van zorgaanbieders voldoen niet aan minimale vereisten.
Het is onduidelijk welke beveiligingsmaatregelen zorgaanbieders voor hun eigen ICT-omgeving hebben getroffen. En welke onderlinge afspraken er zijn gemaakt. Hoe meer partijen, hoe minder controleerbaar en hoe groter het privacyrisico is.

Maatregel:
Samenwerkende zorgaanbieders maken afspraken over welke maatregelen er nodig zijn om COT-leden op een veilige manier gegevens uit te laten wisselen en op te laten nemen in de applicatie LanCOS. Denk aan het gebruik van beveiligde zakelijke laptops, onbeveiligde privélaptops, beveiligde e-mail volgens, in overeenstemming met NTA 7516, gedragscodes, Verklaring omtrent Gedrag, ed.

Verzamelen van de gegevens

De zorgaanbieder meldt een cliënt aan bij een COT. Bij het regisseren van een crisissituatie worden cliëntgegevens door de zorgaanbieder aangeboden aan de crisisregisseur en overige COT-leden. De cliëntgegevens en initiële begeleidende documenten worden via een beveiligde, TLS-encrypted[3] verbinding opgenomen in de applicatie LanCOS. LanCOS is een zelfstandige webversie en heeft geen mogelijkheden om koppelingen te realiseren met andere applicaties.

De zorgaanbieder die een cliënt aanmeldt bij een COT is verantwoordelijk voor een veilige manier van aanleveren van de (bijzondere) persoonsgegevens aan het COT. Hierna is het een gezamenlijke verantwoordelijkheid van COT-leden om zorgvuldig om te gaan met de persoonsgegevens van een cliënt.

Privacyrisico 2: Persoonsgegevens worden overgenomen naar ICT-omgeving zorgaanbieder
Afhankelijk van het 'gebruiksgemak' en dus acceptatie bestaat het risico dat COT-leden bestanden downloaden vanuit de applicatie LanCOS. Of bij het per e-mail rondsturen van documenten deze opslaan binnen hun eigen ICT-omgeving. Dit is strijdig met het uitgangspunt van **dataminimalisatie** vanuit de Algemene Verordening Gegevensbescherming.

Maatregel:
Samenwerkende zorgorganisaties en dus COT-leden hanteren een eenduidige wijze van digitale gegevensoverdracht en spraken af dat (bijzondere) persoonsgegevens van cliënten niet worden opgenomen in hun eigen ICT-omgeving[4].

[3] Op het moment van schrijven van deze DPIA is TLS versie 1.2. van toepassing.
[4] Dit geldt niet voor de COT-zorgaanbieder waarbij de client in zorg is. Deze zorgaanbieder fungeert als 'primaire' verwerkingsverantwoordelijke instelling na het einde van het COT-proces.

Bewaren en vernietigen

In een één-op-één relatie tussen verwerkingsverantwoordelijke (zorgaanbieder) en verwerker (ZorgMatch) kan de verwerkingsverantwoordelijke van de verwerker eisen dat de persoonsgegevens verwijderd worden op het moment dat de dienstverlening eindigt. In het voorbeeld van een COT met meerdere zorgaanbieders kan dat niet. Daar zijn duidelijke afspraken over gemaakt in de verwerkersovereenkomst zoals elke zorgaanbieder die afsluit met ZorgMatch. In een bijlage bij die verwerkersovereenkomst staan bewaartermijnen genoemd:

- Documenten rondom cliënten in een crisissituatie worden tot een half jaar na afloop van de crisissituatie bewaard.[5]
- Overige cliëntgegevens worden tot 7 jaar na afmelding van de crisissituatie bewaard.[6]
- Logging van handelingen door gebruikers in de cliëntgegevens wordt tot 5 jaar na verwijderen van de gebruiker bewaard.

Er staat geen specifieke bewaartermijn genoemd van de gebruikersgegevens zelf.

ZorgMatch verwijdert bovengenoemde cliëntgegevens, tenzij de verwerkingsverantwoordelijke met een schriftelijk verzoek vraagt om deze gegevens langer te bewaren.

Privacyrisico 1: het verwijderen gebeurt niet geautomatiseerd
ZorgMatch heeft nog geen functionaliteit ontwikkeld waarmee in LanCOS geautomatiseerd verwijderd wordt, noch informatie voor verwerkingsverantwoordelijken op basis waarvan zij kunnen zien dat invulling is gegeven aan het verwijderen na afloop van de bewaartermijnen.

Maatregelen:
Ten eerste, zorgaanbieder verzoekt ZorgMatch om het bovenstaande punt – een functionaliteit over een geautomatiseerde wijze van gegevens verwijdering – te ontwikkelen (is al gedaan in fase 1 en is ook toegezegd). Ten tweede, elk COT verzoekt per kwartaal aan ZorgMatch bevestiging dat de oude gegevens verwijderd zijn.

Privacyrisico 2: het verwijderen van gebruikersgegevens
De gebruikersgegevens worden niet verwijderd. Zij worden alleen inactief gemaakt.

Maatregel:
Zorgaanbieder verwijdert zelf de gegevens van gebruiker of verzoekt ZorgMatch dit te doen.

[5] Dit is als standaard maatregel voor dataminimalisatie opgenomen in de applicatie na afsluiting van een crisissituatie/ traject. Documenten zijn opgenomen in medisch/ zorgdossier van client bij eigen zorgaanbieder als verwerkingsverantwoordelijke organisatie.
[6] Vanuit belastingwetgeving geldt een bewaartermijn van zeven (7) jaar voor fiscaal relevante (persoons)gegevens.

Beveiliging

ZN en ZorgMatch hebben bij de ontwikkeling van LanCOS beveiligingsmaatregelen vastgesteld. Op verzoek van ZN heeft KPMG bij ZorgMatch audits uitgevoerd leidend tot een ISAE type 2 rapportage.

LanCOS maakt gebruik van persoonlijke VECOZO certificaten[7] waarmee men op de VECOZO-website of andere websites (zoals LanCOS) kan inloggen in combinatie met verplichte Multi-Factor Authenticatie. Er zijn geen SSO-koppelingen met andere partijen beschikbaar.

Privacyrisico 1: beschikbaarheid software
Op moment van schrijven hebben we nog geen beschikking over de software om zelf de beveiliging te toetsen. Kan een zorgaanbieder zelf bepalen of LanCOS gebruikt mag worden op privéapparaten van medewerkers?

Maatregelen:
Ten eerste, zorgaanbieder test inhoudelijke beveiligingsaspecten voorafgaand aan 'live' gaan met een COT. Ten tweede, ZorgMatch deelt de resultaten van (eventueel nog uit te voeren) beveiligingstests met zorgaanbieders.

[7] https://www.vecozo.nl/support/gebruikers-certificaten-ad/inloggen-wachtwoord/wat-is-single-sign-on-en-hoe-werkt-het/

Inschakelen van een verwerker

ZorgMatch is verwerker voor de verwerkingsverantwoordelijke zorgaanbieders. Dit betreft het beheren van de applicatie LanCOS. VECOZO verzorgt als subverwerker de hosting en het beheer van de infrastructuur waarop LanCOS draait. Dit gebeurt op locaties binnen de EER. In de contractdocumenten is een verwerkersovereenkomst opgenomen die afspraken over deze gegevensverwerking bevat, waaronder:

- ZorgMatch werkt volgens ISO27001/NEN7510
- Gegevens worden uitsluitend verwerkt binnen de EER
- Verwerker gebruikt uitsluitend op naam gestelde accounts, logt gebruik en monitort logging
- Maatregelen op het gebied van detectie zwakke plekken
- Melden datalekken aan verwerkingsverantwoordelijke binnen 24 uur
- Right to audit

Privacyrisico's:
Tijdens het uitvoeren van deze DPIA zijn voor dit aspect geen privacyrisico's naar voren gekomen.

Bronnen

Verwerkersovereenkomst over de levering van LanCOS tussen ZorgMatch BV en [zorgaanbieder].