GEMEENTELIJK DPIA WVGGZ

Algemene effectbeoordeling van de verwerking van persoonsgegevens in de gemeentelijke uitvoering van de Wvggz

VNG

Versie 0.2, 23 december 2019

Inhoudsopgave

1 Inleiding

1.1 Inleiding

Deze DPIA geeft een beschrijving van de verwerking van persoonsgegevens door de gemeente, ten behoeve van de uitvoering van de Wet verplichte geestelijke gezondheidszorg (Wvggz). Bij de verwerkingen is aangegeven wat de grondslag is voor de verwerking, welke privacy risico's er zijn voor de betrokken personen bij de verwerking van hun gegevens, en welke maatregelen de gemeenten, op grond van de AVG en Wvggz-wet, moeten nemen om die risico's te kunnen beheersen.

Op grond van de Algemene Verordening Gegevensbescherming (AVG) is DPIA of een gegevensbeschermingseffectbeoordeling verplicht.[1]

1.2 Aanleiding voor de DPIA

Per 1 januari 2020 is de Wet verplichte geestelijke gezondheidszorg (Wvggz) in werking. De Wvggz is de opvolger van de BOPZ (Wet bijzondere opneming psychiatrische ziekenhuizen). De Wvggz definieert een aantal taken voor (onder anderen) de gemeenten. Om die taken uit te kunnen voeren moet de gemeente persoonsgegevens verwerken. Daarnaast is het op grond van de wet, en voor de juiste uitvoering daarvan, noodzakelijk dat de gemeente persoonsgegevens deelt met andere partijen (o.a. GGZ, politie, Openbaar Ministerie) en met betrokkene zelf, of zijn vertegenwoordiger(s).

In de uitvoering van de Wvggz worden gevoelige persoonsgegevens én bijzondere persoonsgegevens verwerkt van personen in een kwetsbare positie. De beslissingen die de gemeente in de uitvoering van de wet moet nemen, kunnen ingrijpende gevolgen hebben voor betrokkenen, waaronder vrijheidsbeneming of (gedwongen) medisch ingrijpen.

De te verwerken persoonsgegevens bevatten onder andere medische gegevens en mogelijk gegevens over strafrechtelijke veroordelingen en strafbare feiten.

1.3 Algemene effectbeoordeling (art. 35 lid 10 AVG)

Voorliggend document is de DPIA, in de vorm van een algemene effectbeoordeling, op de gemeentelijke uitvoering van de Wvggz.

Met deze algemene effectbeoordeling is een specifieke DPIA door elke individuele gemeente (op grond van art. 35 lid 1 AVG) niet noodzakelijk. Gemeenten kunnen naar deze DPIA verwijzen, en hoeven niet zelf een DPIA uit te voeren op de Wvggz.

De AVG stelt dat bij een nieuwe verwerking de verwerkingsverantwoordelijke een DPIA op de gegevensverwerking moet uitvoeren (art. 35 lid 1 AVG).

[1] De Nederlandse vertaling van de AVG spreekt van een gegevensbeschermingseffectbeoordeling (art. 35 AVG). In de Engelse vertaling is dit een 'dataprotection impact assessment', afgekort DPIA. In dit document zal de term DPIA gebruikt worden.

De AVG regelt verder dat bij een verwerking op grond van een wettelijke plicht of een wettelijke taak voorafgaand aan de invoering van de wet een algemene effectbeoordeling kan worden gedaan (art. 35 lid 10 AVG). Dit betreft dus een verwerking op grond van art. 6 lid 1 sub c of e AVG.

De verwerking van persoonsgegevens in de gemeentelijke uitvoering van de Wvggz is volledig op grond van wettelijke verplichtingen en de uitvoering van wettelijke taken (ofwel: art. 6 lid 1 sub c en e AVG). In het geval van de Wvggz kan daarom worden volstaan met een algemene effect-beoordeling, in de zin van art. 35 lid 10 AVG.

1.4 Totstandkoming van deze DPIA

Veel taken en gegevensverwerkingen zijn in de wetstekst van de Wvggz in detail en specifiek beschreven.

Daarnaast zijn, in samenwerking met het Wvggz Ketenprogramma en vertegenwoordigers van alle ketenpartners, beschrijvingen gemaakt van alle gegevensuitwisselingen die er in de Wvggz zijn, de gegevens die daarbinnen worden uitgewisseld, en de onderliggende informatieproducten.[2]

Zowel in het opstellen van de wet, als in het maken van de informatieproducten zijn de uitgangspunten van privacy-by-design meegenomen. Bij elk informatie-element is gekeken of het noodzakelijk is voor de uitvoering van de gegeven taak, of verwerking noodzakelijk is voor de doelbinding, of het proportioneel is, en of de uit te wisselen gegevens (bij samenwerking tussen ketenpartners) voor de ontvangende partij relevant is.

Voor gemeenten zijn de voorschriften voor de informatieproducten verwerkt in het Khonraad-systeem. Als de gemeente gebruik maakt van het Khonraad-systeem voldoet het aan de afspraken uit de informatieproducten.

De beoordeling van de privacyeffecten in deze DPIA is gemaakt op grond van de wettelijke voorschriften en de met ketenpartners en het ketenprogramma afgesproken informatieproducten. Uit deze beschrijvingen zijn de verwerkingen voor gemeenten, de grondslagen, de gegevens binnen de verwerking, de risico's voor betrokkenen en de maatregelen voor het borgen van de gegevensbescherming af te leiden. Al deze elementen zijn in voorliggende DPIA opgenomen.

De gemeenten hebben in de uitvoering geen beleidsvrijheid om van deze werkwijzen af te wijken.

Op grond hiervan kan de hier voorliggende DPIA dienen als een algemene beoordeling van de privacyeffecten in de zin van art. 35 lid 10 AVG.

Op enkele onderdelen heeft de gemeente wél beleidsvrijheid om de uitvoering naar eigen inzicht in te richten. Bijvoorbeeld: de gemeente kan zelf kiezen waar het Meldpunt voor de Wvggz wordt ingericht, of wie namens de gemeente het Verkennend Onderzoek uitvoert. Deze keuze-mogelijkheden zijn in deze DPIA op de geëigende plaatsen aangegeven.

Dit document is gericht op gemeenten, en de rol van de gemeenten in de uitvoering van de Wvggz.

[2] Zie: https://www.dwangindezorg.nl/uitvoering/wvggz/producten/informatieproducten

In de Wvggz werken gemeenten nauw samen met andere partijen, en zij wisselen daarbij ook persoonsgegevens uit. In deze referentie-DPIA worden die uitwisselmomenten vanuit het perspectief van de gemeenten benoemd.

De beoordeling van de risico's en maatregelen voor de bescherming van persoonsgegevens bij de andere partijen in de Wvggz-keten valt buiten de scope van dit document.

1.5 Verantwoording en beheer

Verantwoording
Dit document is initieel opgesteld door de VNG, oktober 2019

Het document is in de periode oktober-december 2019 gereviewd door:

- een werkgroep van gemeenten (circa 20 gemeentelijke medewerkers: Wvggz deskundigen, FG's van gemeenten, en privacydeskundigen van gemeenten)
- de IBD-gemeenten
- een onafhankelijk privacyjurist
- De FG van de firma Khonraad

De DPIA is opgesteld op basis van het model dat de Gemeentelijke Informatiebeveiligingsdienst (IBD) heeft opgesteld voor een DPIA. Deze DPIA is digitaal beschikbaar in de online tool van de IBD.[3]

Aanpassingen in de komende periode
Deze DPIA is – conform de bedoeling van de AVG – een levend document. In 2020 zijn de volgende aanpassingen voorzien:

- In het eerste kwartaal zal met de gemeentelijke werkgroep een nieuwe review op het document worden gedaan
- De DPIA zal ter review worden voorgelegd aan de Werkgroep Privacy van het Wvggz Ketenprogramma
- De DPIA zal ter review, c.q. ter informatie, aan de Autoriteit Persoonsgegevens worden gezonden
- Eind 2020 zal de DPIA, op basis van de ervaring van gemeenten met de uitvoering van de Wvggz geëvalueerd en waar nodig geactualiseerd en aangepast worden

Beheer en publicatie
Deze DPIA op de Wvggz is nog in ontwikkeling. De meest recente versie (op dit moment: v.0.2) is gepubliceerd op de website van de VNG (www.vng.nl) en van de IBD (www.informatiebeveiligingsdienst.nl)

Opmerkingen en aanvullingen op dit document kunnen gedeeld worden met:

- VNG, Hans Versteeg, hans.versteeg@vng.nl
- IBD, Albert Katoen, albert.katoen@vng.nl

[3] De IBD heeft een online tool ontwikkeld, speciaal voor gemeenten, op basis van de DPIA-tool van de Franse gegevensbeschermingsautoriteit CNIL. Zie: https://pia.informatiebeveiligingsdienst.nl. Om in te loggen is lidmaatschap van de IBD-community noodzakelijk. Zie: https://community.informatiebeveiligingsdienst.nl/

(Tijdelijk) beheer en publicatie van deze DPIA op de Wvggz wordt vooralsnog door de VNG gedaan. In de loop van 2020 zal nader worden bekeken of beheer en publicatie van deze DPIA bij de VNG blijft, wordt overgedragen aan de IBD, of wordt overgedragen aan een andere partij.

Deze DPIA is te vinden in de online DPIA-tool van de IBD onder de naam:
'**sociaaldomein_WVGGZ_DPIA VNG**'

2 Achtergrond bij de DPIA Wvggz

2.1 De Wvggz in het kort

Soms leidt een ernstige psychische aandoening bij iea ertoe dat hij een gevaar voor zichzelf of anderen is. Tot voor kort was een verplichte opname in een instelling de enige manier om deze mensen te helpen en het gevaar weg te nemen.

De nieuwe Wet verplichte geestelijke gezondheidszorg (Wvggz) maakt het mogelijk om verplichte zorg, zoals het toedienen van verplichte medicatie of het uitoefenen van toezicht op betrokkene, poliklinisch of bij iemand thuis te geven. Degene die zorg krijgt, kan dan makkelijker contact blijven houden met familie en vrienden en blijven deelnemen aan de samenleving. Alleen als het in de eigen omgeving echt niet kan, als het er niet veilig genoeg is voor de persoon zelf en zijn omgeving, of de persoon zelf niet wil, kan opname in een instelling een betere oplossing zijn.

De Wvggz biedt zorgverleners meer instrumenten voor zorg op maat. Altijd wordt gekeken naar welke aanpak het beste past bij iemand: verplichte zorg zo kort als mogelijk en zo lang als noodzakelijk.

Bovendien geeft de wet de mensen die verplicht worden behandeld en hun familie meer inspraak. Zij beslissen mee hoe de zorg en ondersteuning eruit gaan zien.

Ook wordt meer dan voorheen met de gemeente gekeken naar wat iemand nodig heeft om deel te (blijven) nemen aan het maatschappelijk leven, zoals een woning en werk. Voor iemand met ernstige psychische problemen is het echter veel beter als we kunnen voorkomen dat het zo slecht gaat dat verplichte behandeling nodig is.

Daarvoor is het noodzakelijk dat alle betrokken partijen en instanties goed samenwerken en signalen van familie, naasten en omgeving in een vroeg stadium opvangen en serieus nemen. Zodat tijdig gestart kan worden met een passende behandeling. Daar wordt niet alleen de patiënt, maar ook de samenleving beter van.[4]

2.2 Hoofdprocessen van de Wvggz

De Wvggz kent twee hoofdprocessen om te komen tot verplichte zorg:

1. Een zorgmachtiging – opgelegd door de rechter
2. Een crisismaatregel – opgelegd door de burgemeester

Daarvan afgeleid kent de Wvggz nog de volgende processen:

3. Het ontvangen van meldingen en doen van een verkennend onderzoek - door de gemeente
4. Een machtiging tot voortzetting van de crisismaatregel - door de rechter
5. Een verzoek zorgmachtiging aansluitend op verlenging crisismaatregel - door de officier van justitie
6. Een beslissing tot tijdelijke verplichte zorg voorafgaand aan een crisismaatregel - door een (daartoe wettelijk bevoegde) zorgverlener
7. Een beslissing tot tijdelijk verplichte zorg in een noodsituatie - door de zorgverantwoordelijke

[4] bron: www.dwangindezorg.nl, 'Kernboodschap Wvggz'

Een zorgmachtiging is een machtiging van de rechter waarmee verplichte zorg toegepast kan worden bij iemand met een psychische stoornis die ernstig nadeel tot gevolg heeft. De rechter verleent een zorgmachtiging alleen als vrijwillige zorg niet mogelijk is, terwijl zorg wel noodzakelijk is om het ernstig nadeel weg te nemen.

Een crisismaatregel is een beslissing van de burgemeester waarmee verplichte zorg toegepast kan worden in een crisissituatie waarin snel ingegrepen moet worden vanwege onmiddellijk dreigend ernstig nadeel. Een crisismaatregel is maximaal drie dagen geldig.

Gemeenten kunnen meldingen ontvangen over personen voor wie de noodzaak tot (mogelijk verplichte) geestelijke gezondheidszorg zou moeten worden onderzocht. De gemeente doet dan een verkennend onderzoek om te bezien of verplichte zorg aan de orde is. Als dat het geval is, dan doet de gemeente een aanvraag voor een zorgmachtiging bij de Officier van Justitie.

2.3 Verwerkingen van persoonsgegevens bij gemeenten

In deze DPIA worden de volgende zes verwerkingen in het kader van de Wvggz bij de gemeenten beschouwd:

Hoofdprocessen Wvggz:

1. Melding en verkennend onderzoek

2. Voorbereiden en uitvoering zorgmachtiging

3. Uitvoeren crisismaatregel (inclusief het ‘horen van betrokkene’)

Ondersteunende processen en randvoorwaarden:

4. Borgen van (Wvggz- en AVG-)rechten van betrokkene

Bedrijfsvoeringsprocessen:

5. Sturingsinformatie, beleidsinformatie en statistiek

6. Autorisatie en registratie van eigen medewerkers

2.4 Beschrijving van de verwerkingen

In Bijlage 1 zijn deze zes verwerkingen in detail beschreven. Per verwerking is aangegeven:

- hoe het verwerkingsproces verloopt,
- wat de wettelijke achtergrond van de verwerking is,
- welke persoonsgegevens verwerkt wordt,
- welke gegevens van andere partijen worden ontvangen,
- welke gegevens aan andere partijen verstrekt moeten worden,
- wat de wettelijke grondslag is voor de verwerking.

De beschrijvingen van de verwerkingen zijn (vanuit de AVG) wettelijk verplicht in een DPIA. Omwille van de leesbaarheid is de beschrijving van de verwerkingen in een aparte bijlage opgenomen. Vanwege de wettelijke verplichting om de verwerkingen in een DPIA te beschrijven is Bijlage 1 een essentieel en integraal onderdeel van deze DPIA.

De zes verwerkingen zijn de basis voor deze DPIA. In de verdere uitwerking van deze DPIA zal steeds aan deze indeling in de zes gemeentelijke verwerkingen gerefereerd worden.

2.5 Noodzaak van een DPIA voor gemeenten

Omdat de Wvggz diverse nieuwe taken en uitvoeringsvereisten bevat ten opzichte van de huidige BOPZ, is de Wvggz te zien als een nieuwe verwerking.

De Wvggz voldoet aan de volgende van de 9 criteria[5] van de WP29[6]:

> 4. Gevoelige gegevens: in de Wvggz worden medische gegevens, en strafrechtelijke gegevens verwerkt
>
> 7. Gegevens van kwetsbare personen: in de Wvggz is in praktisch alle gevallen sprake van verwerking van persoonsgegevens van kwetsbare personen. Op grond van de Wvggz kan de overheid (ingrijpende) inbreuken maken op de vrijheid van personen of op de onaantastbaarheid van het lichaam.

Naast de WP 29 heeft ook de AP een lijst opgesteld van soorten gegevensverwerkingen, waarvoor het uitvoeren van een DPIA verplicht is.[7] De Wvggz omvat de volgende gegevensverwerkingen, die op die lijst zijn genoemd:

> 7. Gezondheidsgegevens
>
> 8. Samenwerkingsverbanden

De Wvggz-wet maakt op diverse plaatsen de gemeente verantwoordelijk voor de verwerking van persoonsgegevens. Onder andere voor het verkennend onderzoek en voor de crisismaatregel heeft de gemeente een wettelijke taak, waarvoor (gevoelige) persoonsgegevens verwerkt moeten worden.

De Wvggz onderkent twee verschillende gemeentelijke partijen, die verwerkingsverantwoordelijk zijn:

- de burgemeester is verantwoordelijk voor de uitvoering van de crisismaatregel
- het college van burgemeester en wethouders is verantwoordelijk voor het ontvangen van meldingen, het verkennend onderzoek en het doen van een aanvraag voor een zorgmachtiging.

Deze gemeentelijke DPIA beschrijft de verwerkingen, grondslagen, risico's en maatregelen van beide verantwoordelijkheden. Waar dat nodig is, zal in de tekst duidelijk onderscheid worden gemaakt tussen de verantwoordelijkheid van de burgemeester of de verantwoordelijkheid van de gemeente (het college van B&W).

---

[5] Zie: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf

[6] De WP29 is de Werkgroep gegevensbescherming artikel 29 (Groep artikel 29). Dit is de onafhankelijke Europese werkgroep die tot 25 mei 2018 (de datum van inwerkingtreding van de algemene verordening gegevensbescherming (AVG)) verantwoordelijk was voor de behandeling van kwesties in verband met de bescherming van de persoonlijke levenssfeer en van persoonsgegevens. De WP 29 heeft op diverse onderdelen van de AVG nadere uitwerkingen gemaakt.

[7] Zie: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667

3 Rollen en verantwoordelijkheden

3.1 Gemeentelijke verwerkingsverantwoordelijkheid

De Wvggz onderscheidt twee categorieën van gemeentelijke verwerkingsverantwoordelijken:

1. De burgemeester, verantwoordelijk voor het opleggen van de crisismaatregel
2. De gemeente (het 'college van burgemeester & wethouders'), verantwoordelijk voor het ontvangen van meldingen, het uitvoeren van het verkennend onderzoek, en het uitvoeren van de ondersteunings- en bedrijfsvoeringsprocessen.

N.B. Als de wet de verantwoordelijkheden formeel neerlegt bij 'het college van burgemeester en wethouders', wordt in deze DPIA in het algemeen gerefereerd aan 'de gemeente'. Waar de verantwoordelijkheid bij de burgemeester ligt, wordt expliciet 'de burgemeester' benoemd.

3.2 Verwerkers

In de uitvoering van de Wvggz zijn er twee categorieën verwerkers voor de gemeenten:

1. Partijen die (delen) van taken voor de gemeente uitvoeren,
2. Gegevensverwerking door derden (ICT-dienstverleners)

Ad 1. Taakuitvoering door derden

De volgende taken laten veel gemeenten door derden uitvoeren:

a. Het ontvangen en verwerken van Wvggz-meldingen
b. Het uitvoeren van het verkennend onderzoek
c. Het horen van betrokkene

Veel gemeenten laten deze taak uitvoeren door de GGD, door een Meldpunt Bezorgd of een Meldpunt Overlast, of een Zorg- en Veiligheidshuis. Het kan zijn dat bovenstaande drie taken bij één partij zijn belegd, of dat taken bij verschillende partijen zijn belegd.

De meldpunten, het verkennend onderzoek en de hoorfunctie zijn in veel gemeenten regionaal georganiseerd. De taakuitvoering gebeurt dan door een derde partij, in opdracht van *een samenwerking tussen gemeenten*.

In alle gevallen dient de opdrachtverstrekking aan de derde goed geregeld te zijn via een delegatie-besluit, of een mandatering (in welk geval er waarschijnlijk ook een verwerkersovereenkomst moet zijn).

N.B. Praktisch alle taken van de burgemeester in de crisismaatregel kunnen alleen gemandateerd worden aan een wethouder, en niet aan andere partijen. De enige twee taken in de crisismaatregel, die wel gemandateerd kunnen worden aan derden zijn het horen, en het opstellen van een beleidsadvies.

Ad 2. Gegevensverwerking door derden

De volgende partijen leveren voor de gemeente (centrale) ICT-diensten:

1. Khonraad (volledig: Khonraad Software Engineering B.V.)

2. Leverancier van veilige mail (in de meeste gevallen: Zivver of Zorgmail)

Met de leveranciers van ICT-diensten moet de gemeente een verwerkersovereenkomst hebben gesloten.

3.3 Noodzaak voor een verwerkersovereenkomst

Als een partij in opdracht van de gemeente (college van B&W of burgemeester) persoonsgegevens verwerkt voor de uitvoering van een (deel)taak, dan moet met die partij een verwerkers-overeenkomst worden gesloten.

Ook hier is het onderscheid van belang tussen:

1. Partijen die (delen) van taken voor de gemeente uitvoeren,
2. Gegevensverwerking door derden (ICT-dienstverleners)

Ad 1. Taakuitvoering door derden

Bij taakuitvoering door derden is het afhankelijk van hoe de opdrachtverlening is georganiseerd, of er wel of niet een verwerkersovereenkomst noodzakelijk is. De AVG vereist een verwerkers-overeenkomst als de verwerkingsverantwoordelijke (de gemeente) beslist over doel en middelen voor de verwerking, maar niet de verwerking zelf doet.

Dit betekent dat als de uitvoerende partij zelf beslist over doel en middelen van de verwerking (lees: zelf de keuze maakt welk ICT-systeem wordt gebruikt, en hoe de registratie gebeurt), dan is de uitvoerende partij de verwerkingsverantwoordelijke geworden, en is er geen verwerkersovereen-komst nodig.

In het algemeen geldt:

- Als de taak (ontvangen van meldingen, verkennend onderzoek, of het horen van betrokkene) **in opdracht** door de derde partij wordt gedaan, dan blijft de verantwoordelijk bij de gemeente, en zal in het algemeen een verwerkersovereenkomst noodzakelijk zijn. De verwerkersovereenkomst kan dan bijvoorbeeld als bijlage bij de opdrachtovereenkomst worden gevoegd.
- Als de taak **in mandaat** door de derde partij wordt gedaan, dan blijft de verantwoordelijkheid eveneens bij de gemeente, en zal in het algemeen een verwerkersovereenkomst noodzakelijk zijn. In het mandaatbesluit kan de gemeente eisen stellen aan de uitvoerder (bijvoorbeeld over de beveiliging van de informatie, of over de manier waarop de partij betrokkenen moet informeren).
- Als de taak **gedelegeerd** wordt uitgevoerd, dan is de verantwoordelijkheid voor de taakuitvoering overgedragen aan de uitvoerende partij. De partij kan dan zelf beslissen over ‘doel en middelen’ voor de gegevensverwerking. En die partij is dan – in de zin van de AVG – de verwerkingsverantwoordelijke. In dat geval is er géén verwerkersovereenkomst noodzakelijk. Omdat de uitvoerende partij zelf verwerkingsverantwoordelijk is, moet zij zelf de verplichtingen vanuit de AVG vervullen (o.a. zorgdragen voor een eigen DPIA, toezicht vanuit een eigen FG organiseren, zorgdragen voor goede informatiebeveiliging, en faciliteren van de AVG-rechten van betrokkenen). De gemeente moet uiteraard wel waarborgen dat de uitvoerende partij voldoet aan de zorgvuldigheidsvereisten vanuit de AVG (zoals informatiebeveiliging, of het correct informeren van betrokkenen). De gemeente kan deze vereisten opnemen in het delegatiebesluit

- Als de uitvoering wordt gedaan door een **gemeenschappelijk regeling** (zoals een GGD) dan beslist de uitvoerende partij over doel en middelen. De verwerkingsverantwoordelijkheid voor de betreffende taak gaat over op de uitvoerende partij, en er is géén verwerkersovereenkomst noodzakelijk. Opnieuw moet de gemeente uiteraard wel eisen stellen aan de zorgvuldigheid van de gegevensverwerking door de GR. Dit kan bijvoorbeeld door een privacyconvenant, door een aanvullende overeenkomst of door aanpassing van de gemeenschappelijke regeling. In het algemeen is de GR-organisatie verwerkingsverantwoordelijk voor al haar taken, en zal zij zelf een eigen privacy-organisatie hebben ingericht, een FG hebben aangesteld, DPIA's uitvoeren e.d.

De vraag of er wel of niet een verwerkersovereenkomst met een uitvoerende derde partij nodig is, is dus sterk afhankelijk van hoe de opdrachtverlening is georganiseerd. Omdat dit per gemeenten en per taak kan verschillen, kunnen hierover in deze DPIA geen specifieke uitspraken worden gedaan. **Het advies aan de gemeenten is om bij dergelijke taakuitvoering door derden advies te vragen aan de eigen FG, of aan een externe privacy-adviseur.** Afhankelijk van de situatie kan specialistisch maatwerk noodzakelijk zijn. Dit valt buiten de scope van deze DPIA (algemene effectbeoordeling).

Ad 2. Gegevensverwerking door derden (ICT-dienstverleners)

Hier gaat het om gegevensverwerking door ICT-leveranciers (Khonraad en leveranciers van veilige mail-voorzieningen).

Met deze partijen moet altijd een verwerkersovereenkomst worden gesloten.

De IBD heeft een standaard verwerkersovereenkomst voor gemeenten ontwikkeld.[8] Het advies is om de overeenkomst met de ICT-leverancier op te stellen aan de hand van dit model.

De IBD is met de firma Khonraad in overleg voor het opstellen van de Khonraad-verwerkersovereenkomst conform de standaard.

3.4 Gezamenlijke verwerkingsverantwoordelijkheid

In de uitvoering van de crisismaatregel werken de gemeente en de GGZ-partijen gezamenlijk in het Khonraad-systeem. In dit geval beslissen gemeente en GGZ dus gezamenlijk over middel voor de gegevensverwerking, en is er sprake van een gezamenlijke verwerkingsverantwoordelijkheid.[9]

In alle andere taken is er wel sprake zijn een gezamenlijke uitvoering, maar géén sprake van een gezamenlijke verwerkingsverantwoordelijkheid. De reden hiervoor is dat de verwerking van de verschillende onderdelen van de taak door de partijen elk in hun eigen systemen wordt gedaan. Elke organisatie beslist zelf over doel en middelen voor hun deel van de gegevensverwerking, en elke partij is dus zelf verwerkingsverantwoordelijk.

[8] Zie: https://www.informatiebeveiligingsdienst.nl/product/handreiking-standaard-verwerkersovereenkomst-gemeenten/

[9] Op grond van Art. 26 lid 1 AVG moeten beide partijen dan een onderlinge regeling opstellen, o.a. over hoe voldaan kan worden aan de rechten van betrokkenen (art. 13 en 14 AVG). Als de wet (in dit geval: de Wvggz) voldoende duidelijk is over de respectievelijke verantwoordelijkheden, dan is de onderlinge regeling niet nodig. Dit is waarschijnlijk de situatie in de Wvggz, maar dit moet nog nader uitgezocht worden. Vanuit de VNG is er nog geen contact hierover geweest met GGZ-Nederland of de NVVP. Daarnaast is nog niet besproken met Khonraad of / hoe dit doorwerkt in de verwerkersovereenkomst van Khonraad met de gemeenten respectievelijk de GGZ-instellingen. Deze punten zal de VNG begin 2020 nader uitzoeken.

Bijvoorbeeld: in de uitvoering van de zorgmachtiging werken de gemeente, de psychiater, de geneesheer-directeur, de officier van justitie en de rechtbank met elkaar samen, maar elke partij doet zijn eigen deel van de gegevensverwerking in het eigen systeem (Khonraad voor de gemeenten). Er is dan geen sprake van gezamenlijke verwerkingsverantwoordelijkheid.

3.5 Locatie van de gegevensverwerkingen

Alle gemeentelijke verwerkingen in de Wvggz (behalve de opslag van de gegevens in het Khonraad-systeem) vinden in Nederland plaats.

- De raadpleging van het Khonraad-systeem vindt plaats op de locatie waar de feitelijke taakuitvoering plaatsvindt (bijvoorbeeld waar de crisismaatregel wordt besloten of waar het verkennend onderzoek plaatsvindt). Dit is altijd in Nederland. N.B. de crisismaatregel wordt altijd besloten door de burgemeester-van-dienst, dus de burgemeester zelf of een locoburgemeester. Als de burgemeester in het buitenland is, is deze taak altijd overgedragen aan een loco-burgemeester, die in de betreffende gemeente zelf aanwezig is.
- Het Khonraad-systeem wordt benaderd vanaf een beveiligde werkplek in de betreffende gemeente (PC, tablet of mobiele telefoon van de burgemeester)
- De verwerking van gegevens via beveiligde mail vindt plaats op de locatie van de gemeente en in de server van de leverancier van de veilige mailvoorziening. In de verwerkersovereenkomst met de leverancier van de voorziening zijn afspraken gemaakt over de locatie van de centrale verwerking.
- Alle overige verwerkingen vinden plaats op de locatie van de gemeente.
- Als taken zijn uitbesteed aan derden (bijvoorbeeld het afhandelen van meldingen of het verkennend onderzoek), dan worden de verwerkingen op locatie van die partij gedaan. In de verwerkersovereenkomst met de derde partij (bij mandatering) of in het delegatiebesluit zijn afspraken opgenomen over de locatie van de verwerking van persoonsgegevens.

Verwerkingen in het Khonraad-systeem kunnen deels buiten Nederland plaatsvinden:

- De verwerkingen in het Khonraad-systeem vinden plaats in een cloud-omgeving, die op meerdere servers (in kopie) draait. Deze redundantie is omwille van de veiligheid en gegarandeerde beschikbaarheid van de ICT-dienst. Khonraad maakt gebruik van servers in het buitenland.[10] In alle gevallen is daarbij geborgd dat de verwerking plaatsvindt conform art. 45 en 46 AVG. De firma Khonraad heeft hierover in de verwerkersovereenkomsten afspraken gemaakt met de leverancier(s) van de cloud-dienst. De gemeente mag (c.q. moet) van de firma Khonraad eisen dat de verwerking op de servers voldoet aan alle beveiligingsvereisten vanuit de AVG. Dit is geregeld in de verwerkersovereenkomst tussen de gemeente en Khonraad.
- Het Khonraad-systeem (en sub-verwerkers van de firma Khonraad) zijn ISO-27001 gecertificeerd, en bij Khonraad is een ISMS (Information security management system) ingericht.[11]

[10] Voor deze DPIA is het niet relevant om welke cloud-diensten het gaat, of in welk land de servers precies staan. In de verwerkersovereenkomst tussen de gemeente en de firma Khonraad wordt hier wel nader op ingegaan. Ook is nadere informatie hierover op verzoek bij de firma Khonraad beschikbaar.
[11] Nadere informatie hierover, inclusief bewijs van de certificering is op aanvraag bij Khonraad te verkrijgen.

- Afgezien van de cloud-diensten van Khonraad, die mogelijkerwijs op servers in het buitenland draaien, vindt er in de uitvoering van de Wvggz géén enkele levering van gegevens plaats over de landsgrenzen heen.

3.6 Verstrekkers van persoonsgegevens aan de gemeente

De volgende partijen verstrekken persoonsgegevens aan de gemeente (college B&W en/of burgemeester) (de verstrekking per partij is in de bijlage in detail verder uitgewerkt en toegelicht)

- Betrokkene
- Zijn vertegenwoordiger(s) / gezinsvoogd
- Zijn advocaat
- De raad voor de rechtsbijstand
- Melder: i) essentiële naaste ii) overige melder
- De zorgverantwoordelijke
- De psychiater die de medische verklaring maakt voor de crisismaatregel
- Geneesheer-directeur
- De GGZ-crisisdienst of ambulancezorg, bij melding van een crisismaatregel
- Politie
- De officier van justitie (openbaar ministerie)
- De rechtbank
- Zorgverleners of andere partijen die (vrijwillige) zorg of ondersteuning leveren aan betrokkene, voor zover van belang bij het verkennend onderzoek

3.7 Ontvangers van persoonsgegevens van de gemeente

De volgende partijen ontvangen persoonsgegevens van de gemeente (college B&W en/of burgemeester) (de ontvangst per partij is in de bijlage in detail verder uitgewerkt en toegelicht)

- Betrokkene
- Zijn vertegenwoordiger(s) / gezinsvoogd
- Zijn advocaat
- De raad voor de rechtsbijstand
- De patiëntvertrouwenspersoon (PVP) en de Stichting PVP
- De familievertrouwenspersoon (FVP) en de Landelijke Stichting Familievertrouwenspersonen
- De tolk (bij het horen)
- Melder (alleen de essentiële naaste)
- De uitvoerder van het verwerken van meldingen (als deze taak is uitbesteed)
- De uitvoerder van het verkennend onderzoek (als deze taak is uitbesteed)
- De zorgverantwoordelijke
- De psychiater die de medische verklaring maakt voor de crisismaatregel
- Geneesheer-directeur
- De GGZ-crisisdienst of ambulancezorg, bij melding van een crisismaatregel
- De partij die het horen doet (als deze taak is uitbesteed)
- Politie
- De officier van justitie (openbaar ministerie)
- De rechtbank

- Zorgverleners of andere partijen die (vrijwillige) zorg of ondersteuning leveren aan betrokkene, voor zover van belang bij het organiseren van vrijwillige zorg of bemoeizorg (als het verkennend onderzoek niet tot een zorgmachtiging leidt)
- Inspectie voor Gezondheidszorg en Jeugd (IGJ)
- Het Rijk (voor beleidsinformatie)
- CBS

3.8 Betrokkenen (in de zin van de AVG)

In de uitvoering van de Wvggz worden over de volgende personen gegevens geregistreerd:

1. De patiënt die (onvrijwillige) zorg ontvangt / moet gaan ontvangen
2. De melder van een melding Wvggz
3. Gemeentelijke medewerkers in de uitvoering (o.a. tbv logging van de gegevensverwerking). N.B. hieronder valt dus ook de (loco-)burgemeester zelf!
4. Medewerkers van partijen die in opdracht van de gemeente een taak uitvoeren (verwerken van meldingen, uitvoeren verkennend onderzoek of 'horen van betrokkene')
5. Vertegenwoordigers van alle in paragraaf 3.6 en 3.7 genoemde partijen (die persoonsgegevens verzenden aan de gemeenten, of ontvangen van de gemeente). Van deze personen worden de contact / identificatiegegevens door de gemeente verwerkt om de in de uitvoering noodzakelijke informatie aan de partij te kunnen sturen.

In de inrichting van het privacybeleid is het van belang om de verschillende categorieën van betrokkenen duidelijk te onderscheiden. Elk van de betrokkenen kan zijn of haar AVG-rechten doen gelden (bijvoorbeeld het recht op inzage), maar in het uitoefenen van het recht van de ene categorie betrokkene, moet de privacy-rechten van de andere categorieën geborgd blijven.
Bijvoorbeeld: een Wvggz-patiënt heeft recht om een Wvggz-melding over hem / haar in te zien, maar de persoonsgegevens van de melder kunnen (als de melder dat wenst), daarbij geanonimiseerd worden. Dit is om de privacy van de *melder* te beschermen. Ook als informatie door de gemeente aan derden is verstrekt heeft de Wvggz-patiënt (in het algemeen) recht om te weten aan welke organisatie (en met welk doel) die informatie is verstrekt, maar aan welke persoon, kán – omwille van de privacy-bescherming van die persoon – geheim worden gehouden.

3.9 Rol functionaris gegevensverwerking van de gemeente

De FG heeft de reguliere rol, die vanuit de AVG is toegekend (zie art. 39 AVG).

3.10 Overige belanghebbenden

Niet van toepassing. Alle bij de uitvoering van de Wvggz betrokken partijen en belanghebbenden zijn in de wet genoemd, en zijn in de opsommingen hierboven en in de beschrijving van de verwerkingen in de bijlage opgenomen. Bovenstaande opsommingen zijn limitatief. Verstrekking van persoonsgegevens aan andere dan de hier genoemde partijen, is in het kader van de uitvoering van de Wvggz, niet aan de orde.

4 Toepasselijke wetgeving en normen

4.1 Welke wetgeving is van toepassing bij de uitvoering van de Wvggz?

Wet Zorg en Dwang (Wzd)
De Wet zorg en dwang is gerelateerd aan de Wvggz. De Wzd regelt de rechten bij onvrijwillige zorg of onvrijwillige opname van mensen met een verstandelijke beperking en mensen met een psychogeriatrische aandoening (zoals dementie). In dat geval is een IBS (inbewaringstelling) mogelijk, die zeer vergelijkbaar is met de crisismaatregel in de Wvgzz. De IBS-WZD wordt tevens via het Khonraad-systeem aan de burgemeester voorgelegd.

Wet Forensiche zorg (WFZ)
De Wet forensische zorg (Wfz) hangt eveneens nauw samen met de Wvggz. De Wfz biedt de officier van justitie en de rechter mogelijkheden om ervoor te zorgen dat binnen het strafrecht sneller de passende psychische zorg wordt geboden. De wet gaat over alle vormen van forensische zorg: ambulant en klinisch, begeleiding en behandeling. De rol van gemeenten in de Wfz is beperkt.

Wet langdurige zorg (Wlz)
De Wet langdurige zorg (Wlz) regelt zware, intensieve zorg voor kwetsbare ouderen, mensen met een handicap en mensen met een psychische aandoening. Als een betrokkene, waarover een melding Wvggz is ontvangen, Wlz-zorg ontvangt, dan is niet de Wvggz van toepassing, maar de Wzd.

Zorgverzekeringswet (Zvw)
De Zvw regelt de verlening van reguliere, verzekerde zorg, waaronder de ggz-zorg. De Wvggz regelt de toegang tot ggz-zorg, in de zin dat de Wvggz niet-vrijwillige zorg mogelijk maakt. De verlening van de feitelijke Wvggz-zorg (psychische hulpverlening), valt onder, en wordt gefinancierd vanuit de Zvw.

Jeugdwet
Als het gaat om ggz-hulpverlening aan jongeren, valt dat niet onder de Zvw, maar onder de Jeugdwet (Jeugd-ggz). In dat geval zijn niet de verzekeraars, maar de gemeenten verantwoordelijk voor de inkoop van de ggz-zorg, en de financiering van de zorgverlening.
Daarnaast is een mogelijk raakvlak met de Wvggz, dat in aanvulling op Wvggz zorg, of als gevolg van een Wvggz-machtiging, jeugdzorg noodzakelijk is. Bijvoorbeeld als een alleenstaande ouder met kinderen, op last van de rechter verplicht in een ggz-instelling verzorgd wordt, dan moet er (vanuit de Jeugdwet) aanvullende zorg zijn voor de kinderen georganiseerd worden.

Wet maatschappelijke ondersteuning (Wmo 2015)
Onder de Wmo vallen onder andere de bemoeizorg en de openbare ggz. Deze vormen van zorg kunnen wellicht toegepast worden ter voorkoming van verplichte ggz. Het is de taak van de gemeente (onder andere in het verkennend onderzoek), om zoveel als mogelijke verplichte ggz te voorkomen, en reguliere (vrijwillige) zorg toe te passen.
Veel gemeenten leggen taken in de uitvoering van de Wvggz (melding, verkennend onderzoek, horen van betrokkene) neer bij een meldpunt bemoeizorg, bij de GGD of een vergelijkbare partij. Deze partijen leveren in het algemeen zorg die onder de Wmo valt. Het is dan van belang dat de taakuitvoering (en de gegevensverwerking!) voor de Wvggz (omwille van de doelbinding) gescheiden blijft van de Wmo-taakuitvoering.

Sociaal domein wetgeving (Jeugdwet, Wmo, participatiewet, wet schuldhulpverlening)
De wetgeving in het sociaal domein regelt diverse vormen van zorg en ondersteuning aan mensen in kwetsbare posities. Ook hier kunnen deze vormen van zorg wellicht toegepast worden ter voorkoming van verplichte ggz. Het is de taak van de gemeente (onder andere in het verkennend onderzoek), om zoveel als mogelijke verplichte ggz te voorkomen, en reguliere (vrijwillige) zorg toe te passen.

Gemeentewet
De gemeentewet beschrijft (onder andere) de taken van de gemeente, en de rolverdeling en verantwoordelijkheidsverdeling tussen de burgemeester en het college van B&W. Beide bestuursorganen hebben een rol in de Wvggz, en het is van belang om hun taken en verantwoordelijkheden te onderscheiden.
Daarnaast heeft de burgemeester vanuit de gemeentewet een taak en bevoegdheid tot de handhaving van de openbare orde en veiligheid (art. 172 Gemeentewet). Dit raakt aan het voorkomen van ernstig nadeel, zoals gedefinieerd in de Wvggz.

Basisregistratie Personen (Wet BRP)
De Wet BRP regelt het gebruik van de identificerende gegevens over personen, en hun woonplaats. Beide onderdelen zijn in de Wvggz van belang. Gemeenten mogen in de Wvggz de BRP raadplegen om de identiteit van betrokkene te verifiëren, en om te bepalen welke gemeente verantwoordelijk is voor de Wvggz-taken ten aanzien van betrokkene (bijv. bij het onderzoeken van meldingen en het verkennend onderzoek, en het doorzetten van een aanvraag voor een zorgmachtiging)

Wet Algemene Bepalingen Burgerservicenummer (WABB) en Wet Burgerservicenummer in de Zorg (Wbsn-z)
De WABB regelt in aanvulling op de Wet BRP het gebruik het burgerservicenummer te identificatie van personen. De Wbsn-z regelt specifiek het gebruik van het BSN in de zorg. In de Wvggz kan het BSN (indien bekend, c.q. beschikbaar) gebruikt worden in de gegevensuitwisseling over betrokkene.

Archiefwet en Burgerlijk Wetboek
De Archiefwet regelt, in combinatie met het Burgerlijk Wetboek, in algemene zin de bewaartermijnen van (overheids)documenten en besluiten. De algemene vereisten vanuit de Archiefwetten gelden ook voor de Wvggz. In de Wvggz is voor de bewaartermijn van de stukken rondom de crisismaatregel aangesloten bij art. 7:454 BW (bewaartermijn van 15 jaar)

Wet geneeskundige behandelovereenkomst (WGBO)
In de WGBO staan de rechten en plichten van cliënten die (medische) zorg krijgen. In het bijzonder is in de WGBO het medisch beroepsgeheim geregeld. Omdat de hulpverlening in de Wvggz valt onder medische zorg, is de WGBO, en alle vereisten ten aanzien van gegevensdeling en geheimhouding van toepassing.

Wet BIG
Het doel van de Wet BIG is te zorgen dat de kwaliteit van onze gezondheidszorg hoog is en blijft. Ook beschermt de Wet BIG patiënten tegen ondeskundig en onzorgvuldig handelen van zorgverleners. Dit doet de Wet BIG onder andere met het BIG-register. Alle medische zorg-verleners in de Wvggz vallen onder de Wet BIG.

Wet Politiegegevens en Wet Justitiële en Strafvorderlijke Gegevens (WJSG)
In de uitvoering van de Wvggz werken de gemeenten (en de ggz) nauw samen met de politie en met justitiële partners. De Wet Politiegegevens regelt de verstrekking en verwerking van persoonsgegevens door de politie. De WJSG regelt de verwerking van justitiële en strafvorderlijke gegevens, door onder het openbaar ministerie en de rechtbank.

Algemene Verordening Gegevensverwerking (AVG) en U-AVG
De AVG is de basis voor de regel aan het verwerken van persoonsgegevens. De Uitvoeringswet AVG (U-AVG) is een nadere toelichting vanuit de Nederlandse wetgever, op de toepassing van de AVG in Nederland. De AVG en de U-AVG zijn beide van toepassing op de gegevensdeling en verwerking van persoonsgegevens in de Wvggz.

4.2 Zijn er normen van toepassing op de gegevensverwerking?

Niet van toepassing. Er zijn geen nadere normen voor de verwerking van persoonsgegevens in het kader van de uitvoering van de Wvggz.

5 Processen, persoonsgegevens en systemen

5.1 Gegevensverwerkingsprocessen in de Wvggz

In bijlage 1 is in detail uitgewerkt welke gegevensverwerkingsprocessen er zijn in de Wvggz, welke persoonsgegevens in die processen worden verwerkt, en welke verstrekkingen er zijn tussen de gemeenten en andere uitvoerders in de Wvggz.

5.2 Welke bijzondere persoonsgegevens worden verwerkt?

In de Wvggz worden door de gemeente de volgende categorieën van bijzondere persoonsgegevens verwerkt:

- Medische gegevens (o.a. psychische stoornis of vermoeden daarvan)
- Politiegegevens
- Justitiële en strafvorderlijke gegevens
- Historie verplichte zorg

In de bijlage is in detail opgenomen welke gegevens, in welke processen worden verwerkt. Daarbij is ook de verwerking van de bijzondere persoonsgegevens aangegeven, inclusief de grondslag voor die verwerking.

Omdat in de Wvggz bijzondere persoonsgegevens worden verwerkt, is extra aandacht nodig voor de risico's die daaraan vast zitten. In de hoofdstukken risico's (hoofdstuk 9) en de maatregelen (hoofdstuk 10) wordt hier nader op ingegaan.

5.3 Systemen voor gegevensverwerking

In de gegevensverwerking binnen de Wvggz gebruiken de gemeente de volgende ICT-systemen:

5.3.1 Khonraad Wvggz-systeem

Khonraad is het primaire processysteem de uitvoering van de Wvggz door gemeenten.

Het systeem ondersteunt de gemeente bij de volgende verwerkingen:

- Melding
- Verkennend onderzoek
- Horen van betrokkene
- Beslissing crisismaatregel
- Doorzetten aanvraag tot zorgmachtiging naar de officier van justitie

In de bijlage is in meer detail een beschrijving gegeven van de gegevensverwerkingen in het Khonraad-systeem.

Tussen de (koepels van) ketenpartijen in de Wvggz zijn afspraken gemaakt over gestandaardiseerde informatieproducten. In het Khonraad-systeem zijn de standaarden ingebouwd. Door gebruik te maken van het systeem wordt voldaan aan de vereisten van de standaard informatieproducten.

De logging van alle acties door gebruikers in het systeem wordt vastgelegd. Hierdoor kan worden voldaan aan de informatieverplichtingen richting betrokkenen op grond van de AVG. De logging (niet alleen van medewerkers, maar ook van tijdstippen van handelingen) is daarnaast van belang voor de

termijn-bewaking van activiteiten, die op grond van de Wvggz verplicht is. Het systeem geeft automatisch een bericht aan gebruikers als termijnen dreigen overschreden te gaan worden.

Daarnaast ondersteund het systeem bij het volgen van work-flows, die op grond van de Wvggz verplicht zijn. Bijvoorbeeld: om een crisismaatregel te kunnen besluiten moet er een medische verklaring zijn opgesteld, moet betrokkene gehoord zijn, en moeten enkele aanvullende gegevens gecheckt zijn (zoals geen bezwaar tegen toevoeging van een advocaat, of informeren van de pvp / fvp). Het Khonraad-systeem checkt automatisch of voldaan is aan de te volgen stappen vanuit de wet, en of voldaan is aan de vereisten ten aanzien van een volledig dossier. Daarbij checkt het systeem of noodzakelijke gegevens aanwezig zijn, en verhinderd het systeem dat ander (voor de casus niet relevante) gegevens worden toegevoegd. Op deze manier wordt invulling gegeven aan 'privacy-by-design' (art. 25 AVG).

5.3.2 Veilige mailvoorziening

Voor alle niet-geprotocoleerde gegevensuitwisselingen en registraties wordt in de uitvoering van de Wvggz gebruik gemaakt van een veilige e-mailvoorziening. Het gaat dan bijvoorbeeld om vragen over nadere informatie, overleg tussen partijen e.d. Het gaat dan om gegevensuitwisseling die niet via het Khonraad is voorzien.

Omdat de Wvggz in detail regelt welke informatie tussen partijen gedeeld kan worden, en omdat het Khonraad-systeem op basis van de wet gebouwd is, is het de bedoeling dat het gebruik van veilige mail tot het minimum wordt beperkt.

Het gebruik van een niet-veilige mail-voorziening voor de uitwisseling van persoonsgegevens in de uitvoering van de Wvggz is niet toegestaan.

De veilige mailvoorziening moet voldoen aan de NTA 7516.[12] Deze norm is door het NEN en door het ministerie van VWS ontwikkeld voor de toepassing van veilige e-mail in de zorg.

Op grond van de afspraken tussen de ketenpartijen is gebruik van veilige mail (conform de NTA) verplicht voor alle gemeenten, en alle partijen die taken in opdracht van de gemeente uitvoeren.

De meest gebruikte voorzieningen voor veilige mail bij de gemeenten zijn Zivver en Zorgmail.

In het Khonraad-systeem is ook een berichtenbox aanwezig. Deze berichtenbox is niet een veilige mailvoorziening (zoals Zivver of Zorgmail), maar de box voldoet wel aan de vereisten van de NTA 7516.

5.3.3 Overige systemen bij uitvoerende derden

Veel gemeenten hebben delen van de uitvoering van de Wvggz belegd bij derden. Het gaat dan met namen om het ontvangen van meldingen, het uitvoeren van het verkennend onderzoek en het horen van betrokkene (bij de crisismaatregel).

Het is mogelijk dat die partijen besluiten om hun deel van de taakuitvoering te doen in de systemen, die ze voor andere taken al beschikbaar hebben.[13]

[12] Zie: https://www.nen.nl/Alles-over-NEN-7510/NTA-7516.htm

[13] De vraag is of dit handig is. In het Khonraad-systeem is functionaliteit aanwezig voor de veelal uitbestede taken. Omdat de melding, het verkennend onderzoek en het horen onderdeel zijn van de andere werkstromen in de Wvggz (zorgmachtiging, respectievelijk crisismaatregel) moet op enig moment door de partijen of doorde gemeente alsnog de melding, de resultaten van het verkennend onderzoek of het hoorverslag in Khonraad aan

Registratie van de persoonsgegevens gebeurt dan in de systemen van de derde partij. Voorkomende systemen zijn:

- GGD, registratie in Clavis
- Zorg- en Veiligheidshuis, registratie in GCOS
- Andere partij / registratie op eigen manier, bijvoorbeeld in Word-documenten of Excellijsten.

In dergelijke gevallen moet de gemeente in op de opdrachtomschrijving aan de derde partij, c.q. in de verwerkersvereenkomst eisen opnemen aan de systemen waarin de derde partij de persoonsgegevens verwerkt. Eisen zijn in elk geval:

- Dezelfde eisen aan de informatiebeveiliging, die ook gelden voor de gemeente, namelijk de Baseline Informatiebeveiliging Overheid (BIO v1.03)[14]
- Registratie in het systeem dient – via autorisaties of anderszins – afgeschermd te zijn van andere registraties die de organisatie doet (bijvoorbeeld als de GGD de meldingen Wvggz doet, moeten die gescheiden geregistreerd worden van de meldingen voor zorg & overlast, of de meldingen bemoeizorg)
- Medewerkers die de Wvggz uitvoeren hebben voor de registratie aparte autorisaties, rollen en profielen in het systeem (ten opzichte van andere (niet-Wvggz) taken, die de organisatie eventueel ook in het systeem registreert)
- Gebruik van veilige mail, conform NTA 7516, van alle overige communicatie met de gemeente en andere partijen in het kader van de Wvggz.

5.4 Andere vormen van gegevensverwerking in de Wvggz

Alle verwerkingen in de Wvggz betreffen:

- Vastlegging en raadpleging van de gegevens
- Delen van gegevens (ontvangen van en verstrekken aan betrokkenen partijen en Wvggz ketenpartners)

Alle registraties zijn op basis van de individuele casus (melding, verkennend onderzoek, crisismaatregel, zorgmachtiging)

Voor de volledigheid zij opgemerkt, dat in de uitvoering van de Wvggz er **géén is** sprake van:

- Grootschalige verwerking of analyse van databestanden op persoonsniveau
- (Semi-) geautomatiseerde besluitvorming
- Profiling
- Big-dataverwerking
- Gebruik van algoritmen

Bij dergelijke verwerkingen stelt de AVG nadere eisen, maar die zijn voor de Wvggz dus niet van toepassing.

---

het dossier worden toegevoegd. Er is op dit moment geen systeemkoppeling beschikbaar tussen Khonraad en de andere systemen, waardoor de gegevens moeten worden overgetypt. Dit leidt tot extra werk, maar ook tot extra risico's in de informatiebeveiliging en de informatieintegriteit.

[14] zie: https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/

6 Grondslag voor de gegevensverwerking

In de bijlage is voor elke gegevensverwerking in detail opgenomen wat de grondslag is voor de verwerking.

Daarnaast is vanuit het Ketenprogramma Wvggz een inventarisatie gemaakt van de privacy-aspecten van de wet. De grondslagen voor de verwerkingen in de Wvggz (voor de gemeenten, én voor de andere partijen) zijn toegelicht in de Privacy-Handreiking Wvggz, Ketenprogramma implementatie Wvggz, Werkgroep BSN / privacy Wvggz, versie 0.8, d.d. 27-06-2019.[15]

6.1 Grondslag in het algemeen

De verwerkingen die de gemeente (zowel burgemeester als college B&W) doet, op grond van de Wvggz, zijn in beginsel op basis van de volgende twee grondslagen:

- De verwerking (en/of verstrekking) is noodzakelijk voor een taak van algemeen belang of voor een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen, die bij wet (te weten de Wvggz) is voorzien (art. 6 lid 1 sub e AVG) en/of
- De verwerking (en/of verstrekking) is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust (opgenomen in de Wvggz) (art. 6 lid 1 sub c AVG).

Voor beide grondslagen gelden verder de volgende eisen:

- De rechtsgrond voor de bedoelde verwerking moet worden vastgesteld bij unierecht of lidstatelijk recht
- Het doel van de verwerking wordt in die rechtsgrond vastgesteld of is met betrekking tot de in art 6 lid 1 e AVG bedoelde verwerking noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend.

Voor alle taken en wettelijke verplichtingen die in deze handreiking staan opgenomen, geldt dat zij in de Wvggz staan. In de bijlage is voor elke gegevensverwerking in detail aangegeven op grond van welke artikel in de Wvggz de verwerking verplicht of toegestaan is. Daarmee wordt in beginsel voldaan aan de eerste aanvullende eis.

Voor de tweede aanvullende eis geldt dat het doel van de verwerking niet expliciet in de rechtsgrond hoeft te zijn opgenomen of vastgesteld. Zie hiervoor bijvoorbeeld overweging 41 AVG. De rechtsgrond moet echter wel duidelijk en nauwkeurig zijn, en de toepassing moet voorspelbaar zijn voor betrokkene. Met specificatie van alle taken en verwerkingen in de Wvggz-wetstekst is hieraan voldaan. In de bijlage is deze specificatie van taken en verwerkingen beschreven.

[15] Zie https://www.dwangindezorg.nl/uitvoering/documenten/publicaties/implementatie/ketenproducten/producten-wvggz/concepthandreiking-privacy-v0.8

6.2 Gebruik van toestemming

Toestemming als grond voor het verwerken van persoonsgegevens (art. 6 lid 1 a AVG) is in de Wvggz eigenlijk niet aan de orde. In de Wvggz is in detail geregeld welke informatie over betrokkene (met name de betrokken patiënt voor de verplichte zorg) mag worden geregistreerd.

Verstrekking van persoonsgegevens op basis van toestemming staat op gespannen voet met de verplichting die op diverse plekken in de Wvggz onderliggend is. Hierdoor is het moeilijk om te borgen dat de toestemming door betrokkene vrij, en zonder last is verstrekt. Om deze reden heeft de wetgever besloten in de Wvggz praktisch geen gebruik te maken van toestemming als grondslag voor de gegevensverwerking.

In algemene zin geldt in de Wvggz: als de gegevens verstrekt kunnen worden, dan moet de verstrekking ook, op grond van de wet. Als verstrekking achterwege kan blijven, dan is de verstrekking ook niet toegestaan op grond van de wet. Dit is conform het beginsel van dataminimalisatie (art. 5 lid 1 sub c AVG).

Op enkele plekken is er in de Wvggz – in meer of mindere mate – sprake van een vorm van toestemming:

- In de Wvggz is de uitdrukkelijke toestemming van betrokkene nodig, voor het verstrekken van persoonsgegevens aan de patiëntvertrouwenspersoon of de familievertrouwenspersoon.
- In de praktische uitvoering van de Wvggz is afgesproken dat de expliciete toestemming van betrokkene wordt gevraagd bij met maken van een audio-opname van het hoorverslag. De toestemming wordt ook gevraagd voor het het delen van die audio-opname met de burgemeester.
- Een melder kan aangeven dat een melding anoniem wordt verwerkt. Dat betekent dat gegevens over de melder niet met anderen (en in het bijzonder: niet met de patiënt voor verplichte zorg) kunnen worden gedeeld. Dat zou kunnen worden gezien als gebruik van toestemming door de melder voor het verstrekken van zijn persoonsgegevens. De verwerking van een anonieme melding werkt echter op meer plekken in de wet verder door (bijvoorbeeld de anonieme melder heeft dan ook het recht om anoniem door de rechter gehoord te worden), dat in de praktijk eerder sprake is van een wettelijke taak (art. 6 lid 1 sub e AVG) dan van toestemming (art. 6 lid 1 sub a AVG).
- Betrokkene kan de toevoeging van een advocaat - en de daarbij behorende verwerking van persoonsgegevens - weigeren (art. 7:2 lid 3 Wvgzz)
- Betrokkene kan weigeren gehoord te worden (art. 7:1 lid 3 sub b Wvggz)

6.3 Geheimhoudingsplicht Wvggz

De Wvggz kent voor de betrokken uitvoerders, waaronder de burgemeester en het college van B&W een geheimhoudingsplicht (art. 8:34 Wvggz). Als taken door de burgemeester of het college van B&W aan derden zijn opgedragen (zoals het verwerken van meldingen, het verkennend onderzoek of het horen) dan geldt de geheimhoudingsplicht dus ook voor die partijen.

Daarnaast geldt de geheimhoudingsplicht, die de medische professionals op grond van de WGBO hebben (medisch beroepsgeheim).

De geheimhoudingsplicht van de Wvggz en de geheimhoudingsplicht van het medisch beroepsgeheim staan naast elkaar en gelden allebei tegelijkertijd. Dat betekent dat er voor een verstrekking voor beide vormen van geheimhouding een grond moet zijn om het beroepsgeheim te

kunnen doorbreken. In alle informatieverplichtingen in de Wvggz is die grond gegeven. Als in de Wvggz op grond van een specifieke taak gegevens over betrokkene gedeeld *mogen* worden, dan *moet* het in het algemeen ook.

6.4 Grondslag voor verwerking medische gegevens

Bij de verwerking van bijzondere categorieën van persoonsgegevens, zoals gegevens over de gezondheid, moet er naast de grondslag voor de verwerking van persoonsgegevens uit artikel 6 AVG, ook een uitzondering van toepassing zijn op het verbod op het verwerken van bijzondere categorieën van persoonsgegevens. Deze uitzonderingen staan opgenomen in art. 9 lid 2 AVG en zijn deels verder uitgewerkt in de U-AVG.

Sommige uitzonderingen zijn rechtstreeks toepasselijk op basis van de verordening. Het gaat hier om de onderdelen a, c, d, e en f. Voor andere uitzonderingen is dit in de specifieke wetsartikelen in de WVggz geregeld. (voor de onderdelen b, g, h, i en j.

1. Een belangrijke uitzonderingsgrond voor de verwerking van gegevens over de gezondheid in het kader van de Wvggz, is volgens de wetgever gelegen in art. 9 lid 2 sub g AVG: de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht (…)', te weten de Wvggz. Volgens de wetgever 'zijn dit wetsvoorstel en de introductie van de commissie ingegeven door het belang om gedwongen zorg aan personen met een psychische stoornis zoveel mogelijk te beperken. Het behoeft geen betoog dat dit belang als een zwaarwegend algemeen belang is te kwalificeren'. Daarbij is het wel van belang dat:
    i) de evenredigheid met het nagestreefde doel wordt gewaarborgd,
    ii) de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en
    iii) passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.

    In de memorie van toelichting bij de Wvggz staat daarover onder andere het volgende: 'De systematiek van de wet, de algemene uitgangspunten van hoofdstuk 2, de rechterlijke toetsing vooraf, de specifieke bepalingen ten aanzien van het zorgplan (artikel 5:8), de zorgmachtiging (6:3) en de crisismaatregel, het gebruik van richtlijnen (artikel 8:3 ev) en de zorgvuldigheidseisen bij tijdelijke verplichte zorg in onvoorziene situaties (artikel 8:9) bieden gezamenlijk de waarborg dat de zorgvuldigheidseisen die artikel 27 van de Aanbeveling (van de Raad van Europa Recommendation 10 (2004) concerning the protection of the Human Rights and Dignity of Persons with Mental Disorder) stelt, in de praktijk worden geëffectueerd'.

2. Voor zorgverleners lijkt een alternatieve uitzonderingsgrondslag op het verwerkingsverbod van gegevens over de gezondheid gelegen in art. 9 lid 2 sub h AVG jo art. art. 22 UAVG jo art. 30 lid 3 sub a UAVG: ((…) 'het verbod om gegevens over gezondheid te verwerken is niet van toepassing indien de verwerking geschiedt door hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene' (…)).

Omdat de gemeente geen onderdeel is van de behandeling (de gemeente verwerkt alleen de melding en de burgemeester neemt de beslissing tot de crisismaatregel) is deze grondslag voor de gemeenten niet van toepassing.

3. Ketenpartners kunnen volgens de wetgever ook op grond van art. 5 EVRM verplicht worden tot het overleggen van medische gegevens. In de MvT bij de Wvggz staat: 'Artikel 5 EVRM brengt mee dat de beslissing om iemand van zijn vrijheid te benemen wegens een geestesstoornis gestoeld moet zijn op een medisch-deskundig oordeel over de actuele gezondheidstoestand van de patiënt. De medische verklaring en het zorgplan in de artikelen 5:6 en 5:8 geven hier (mede) uitvoering aan. Overhandiging van deze documenten aan de commissie valt weliswaar onder het verbod van artikel 16 Wbp, maar wordt gerechtvaardigd door de naleving van volkenrechtelijke verplichtingen, zoals het EVRM (artikel 23, eerste lid, onder d, Wbp)'.

Kortom, ondanks dat de commissie uit het Wvggz-wet is verdwenen en de Wbp is vervangen door de AVG, kan worden gesteld dat art. 5:17 lid 3 Wvggz jo art. 5 EVRM jo art. 23 sub a UAVG de officier van justitie bijvoorbeeld verplicht om gegevens betreffende de gezondheid aan het verzoekschrift voor de afgifte van een zorgmachtiging toe te voegen, omdat art. 5 EVRM met zich brengt dat de beslissing om iemand van zijn vrijheid te benemen wegens een geestesstoornis, gestoeld moet zijn op een medisch-deskundig oordeel over de actuele gezondheidstoestand van de patiënt. Omdat deze verwerking/verstrekking noodzakelijk is om te voldoen aan een volkenrechtelijke verplichting, is op grond van art. 23 sub a UAVG het verbod om bijzondere categorieën van persoonsgegevens te verwerken in dit geval niet van toepassing.

Voor de gemeente is deze uitzondering relevant, omdat het de grondslag biedt waarop de burgemeester de gegevens over de medische verklaring mag (c.q. moet) ontvangen en verwerken bij het beslissen over een crisismaatregel. De burgemeester moet immers vast kunnen stellen dat de beoordeling is gebaseerd op een medische-deskundig oordeel.

6.5 Grondslag voor de verwerking strafrechtelijke gegevens

Grondslag

Artikel 10 van de AVG biedt ruimte om, binnen het domein van de verordening (dus daar waar geen sprake is van verwerking met het oogmerk opsporen en vervolgen), gegevens van strafrechtelijke aard te verwerken, mits dit geschiedt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen, die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden.

Anders dan onder de Wbp zijn persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten onder de AVG/UAVG niet meer aangemerkt als bijzondere categorieën van persoonsgegevens. De AVG biedt echter ruimte aan de nationale wetgever om uitzonderingen aan te brengen op het verbod om persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten te verwerken.

De artikelen 31, 32 en 33 van de UAVG zijn een uitwerking van de mogelijkheid die artikel 10 van de verordening biedt om de verwerking van persoonsgegevens van strafrechtelijke aard toe te staan bij lidstaat-rechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden.

Vuistregels voor de verwerking van strafrechtelijke en justitiële gegevens

Voor de verwerking van gegevens van strafrechtelijke aard in het kader van de Wvggz, lijken in het bijzonder de volgend uitzonderingsgronden van belang:

1. de verwerking noodzakelijk is in aanvulling op de verwerking van gegevens over gezondheid, bedoeld in artikel 30, derde lid, aanhef en onderdeel a, met het oog op een goede behandeling of verzorging van de betrokkene (art. 33 lid 1 sub c UAVG).
2. De verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang (‘noodzakelijk ter voldoening aan een volkenrechtelijke verplichting’, bijvoorbeeld art. 5 EVRM) als bedoeld in artikel 23 sub a AVG (art. 32 sub e UAVG).

Let op: Ook hier geldt dat de gemeente geen onderdeel van de behandeling, of de uitvoering van de crisismaatregel / zorgmachtiging is. De gemeente mag dus alleen de gegevens ontvangen, die noodzakelijk zijn om de crisismaatregel te kunnen beslissen, of gegevens die in het verkennend onderzoek van belang zijn. De Wvggz geeft in de wet expliciet aan welke gegevens de gemeente daarvoor mag gebruiken.

7 Toepassing van de AVG-beginselen (art. 5 AVG)

7.1 Rechtmatigheid, behoorlijkheid en transparantie

In de Wvggz zijn de doelen van de verwerking in detail gespecificeerd en expliciet gemaakt.

De verwerkingsdoelen van alle verwerkingen vinden hun grondslag in de Wvggz.

Daarbij geldt dat de verwerking is op grond van een wettelijke verplichting of de verwerking is noodzakelijk voor een taak van algemeen belang (art. 6 lid 1 sub c of sub e AVG).

In de bijlage is voor alle verwerkingen in detail opgenomen welke persoonsgegevens voor dat proces verwerkt worden, en wat daarbij de grondslag is. De verwerkingsdoelen zijn beschreven onder 'overzicht' in het hoofdstuk 'context'.

Daarmee is voor alle betrokkenen inzichtelijk welke persoonsgegevens worden verwerkt, met welk doel en dat dat doel rechtmatig is. Door de mate van detail in de Wvggz is de opsomming van verwerkingen en verstrekking limitatief. Voor betrokkenen is dan duidelijk dat als een verwerking niet in de Wvggz is genoemd, dat de verwerking ook niet is toegestaan.

Alle gegevensproducten voor de Wvggz zijn beoordeeld in een werkgroep, waarin alle ketenpartners hebben deelgenomen (OM, politie, gemeenten, GGZ, advocatuur), alsmede een vertegenwoordiging vanuit de cliëntenorganisaties (MIND).

In deze werkgroepen is per gegevens element in de informatieproducten bekeken:

- of er een wettelijke noodzaak is om het gegevenselement op te nemen
- of verwerking, danwel verstrekking of ontvangst voor de betreffende partij strikt noodzakelijk is
- of – bij voorkeur – de verwerking is terug te voeren op een wettelijke plicht (de Wvggz vermeld op diverse plekken expliciet welke gegevens op welk moment tussen welke partijen gedeeld mogen worden)
- of de verwerking door de betreffende partij proportioneel is

Om te kunnen voldoen aan de vereisten van behoorlijkheid en transparantie zijn verder de informatieproducten van belang. De rechtmatigheid, behoorlijkheid en de bijdrage van de informatieproducten aan de transparantie zijn beoordeeld in de eerder genoemde rapportage 'Werkgroep BSN / Privacy Wvggz'.

Omdat de informatieproducten openbaar zijn gepubliceerd is voor betrokkene vooraf na te gaan welke persoonsgegevens op welk moment in de uitvoering van de Wvggz exact worden verwerkt.

De in de informatieproducten afgesproken gegevensverwerkingen zijn opgenomen in het Khonraad-systeem. Als gemeenten gebruik maken van het Khonraad-systeem kunnen dus alleen de gegevens verwerkt worden, die in de werkgroepen als proportioneel en relevant zijn beoordeeld.

7.2 Doelbinding

In de bijlage is voor elke verwerking in aangegeven welke persoonsgegevens worden verwerkt en wat de doelen van de verwerking zijn. Daarnaast is in de beschrijving van de verwerking nader toegelicht hoe de te verwerken persoonsgegevens noodzakelijk zijn voor het behalen van de doelen van de verwerking.

7.3 Gegevensminimalisatie

In de bijlage is per verwerking een opsomming opgenomen van de te verwerken persoonsgegevens.

Voor alle gegevens geldt dat er:

- ofwel een wettelijke plicht is om ze te verwerken (art. 6 lid 1 sub c AVG)
- ofwel de verwerking noodzakelijk is voor de uitvoering van de betreffende taak van algemeen belang in de Wvggz (art. 6 lid 1 sub e AVG)

Om aan de vereisten van proportionaliteit en dataminimalisatie te voldoen zijn opnieuw de door de ketenpartijen vastgestelde standaard informatieproducten van belang. Om te kunnen voldoen aan de vereiste van dataminimalisatie is dan wel noodzakelijk, dat de gemeente in de uitvoering van de Wvggz zich houdt aan de volgende afspraken, c.q. wettelijke vereisten:

- Gebruik maken van een ICT-systeem dat gebaseerd is op de informatieproducten (dit geldt voor het Khonraad-systeem)
- Gebruik maken van beveiligde mail (die voldoet aan de NTA 7516), voor de overige verstrekking van persoonsgegevens
- De overige communicatie tot het strikt minimale beperken
- De gegevens, die partijen in de uitvoering van de Wvggz ontvangen of verwerken, worden niet gebruiken voor andere doeleinden (doelbinding). In het bijzonder: uitvoerders van gemeentelijke taken (melding, verkennend onderzoek, horen) zorgen dat de registratie van de persoonsgegevens voor die Wvggz-taken, gescheiden is van de registratie van persoonsgegevens voor andere taken die zij uitvoeren.

7.4 Actualiteit en juistheid van de persoonsgegevens

In de Wvggz zijn er drie mechanismen die zorgen dat gegevens zoveel als mogelijk actueel en juist zijn.

1. De uitvoering van de Wvggz is casusgericht.

Dat wil zeggen: de uitvoering is gericht op het verzamelen van actuele gegevens over betrokkene, zijn situatie, mogelijke zorg e.d., en op basis daarvan een beslissing nemen. Voor elke casus wordt in beginsel het hele dossier op dit moment verzameld.

De twee hoofdprocessen in de Wvggz zijn:

- Zorgmachtiging
- Crisismaatregel

De gegevens, die voor beide maatregelen worden verzameld en verwerkt, worden specifiek voor de beslissing over die maatregel verzameld. Daarbij kan weliswaar worden voortgebouwd op informatie

die in databases aanwezig is (bijvoorbeeld de historie van verplichte zorg bij het Openbaar Ministerie), maar ook dan wordt die informatie voor de actuele casus geverifieerd en getoetst aan de actuele situatie van betrokkene

2. Op diverse plekken in de uitvoering van de Wvggz zitten controles van de juistheid van de gegevens ingebouwd.

In de uitvoering werken partijen (met name: gemeente / burgemeester, psychiater, geneesheer-directeur, officier van justitie, politie en zorgverlener) nauw met elkaar samen. Ingrijpende besluiten worden door bevoegd gezag genomen (de burgemeester voor een crisismaatregel, de rechter voor het verlengen van een crisismaatregel en de zorgmachtiging). In de voorbereiding van dat besluit werken meerdere partijen mee, waarbij iedereen steeds de inhoud van de dossieropbouw kan controleren.
Bijvoorbeeld: in de crisismaatregel wordt de medische verklaring opgesteld door de psychiater. Die overlegt daarvoor eventueel met de burgemeester. De burgemeester beoordeelt de medische verklaring voordat hij de crisismaatregel neemt. De crisismaatregel, inclusief de medische verklaring wordt vervolgens gedeeld met o.a. de geneesheer-directeur, de betrokkene, zijn advocaat, en de Inspectie Gezondheidszorg en Jeugd. Bovendien heeft betrokkene een recht op beroep, en kan hij (of zijn advocaat) bij onjuiste informatie in de crisismaatregel het besluit door de burgemeester waarschijnlijk met succes bij de rechter aanvechten.
Die zorgvuldigheid, en samenwerking tussen partijen in de totstandkoming van de informatiepositie, is in de wet met opzet opgenomen. Dit is juist zo geregeld, omdat de inbreuk van verplichte zorg een zeer grote impact kan hebben voor betrokkene, en het daarmee van deste groter belang is om de juistheid van de gegevens te kunnen borgen.

3. De betrokkene of zijn vertegenwoordiger(s) wordt op diverse plaatsen in de wet bij de uitvoering betrokken, en kan aangeven of gegevens niet correct zijn.

De manieren waarop de betrokkene zijn rechten kan borgen zijn onder andere:

- De toevoeging van een advocaat
- Ondersteuning door een patiënt vertrouwenspersoon (PVP)
- De mogelijkheid om gehoord te worden (bij een crisismaatregel)
- Een zitting bij de rechter (bij een zorgmachtiging)
- De mogelijkheid van beroep op een beslissing
- Toezicht op de uitvoering door de geneesheer-directeur
- Toezicht op de uitvoering door de IGJ

De details van welke persoonsgegevens worden verwerkt, welke partijen daarbij betrokken zijn, op welk moment zij elkaar informeren en wie daar uiteindelijk een besluit op baseert is in de bijlage uitvoering beschreven, en wordt hier niet herhaald.

7.5 Bewaartermijnen

De bewaartermijnen zijn geregeld in art. 8:32 en 8:33 Wvggz.

- Zorgmachtigingen en crisismaatregelen worden in beginsel 15 jaar bewaard, conform art. 7:454 lid 3 BW.

- Betrokkene kan na 5 jaar een verzoek tot vernietiging doen, als het verzoek wordt toegewezen moet het dossier binnen maximaal 3 maanden worden vernietigd.

7.6 Informatiebeveiliging en gegevensintegriteit

De Wvggz stelt geen technische eisen aan de informatie-systemen.

In de nadere afspraken tussen ketenpartijen, en in de afspraken die gemeenten onderling hebben gemaakt over informatiebeveiliging, zijn er wel standaarden van toepassing:

- Voor de informatiebeveiliging van gemeentelijke verwerking geldt dat die moet voldoen aan de Baseline Informatiebeveiliging Overheid (BIO v1.03). [16] De BIO wordt voor gemeenten onderhouden en beheerd door de Informatiebeveiligingsdienst gemeenten. Toepassing van de BIO is voor gemeenten verplicht op grond van de 'Circulaire toepassen Baseline Informatiebeveiliging Overheid in het digitale verkeer met het Rijk'.[17]
- Voor het gebruik van Veilige Mail geldt dat de mailvoorziening moet voldoen aan de NTA 7516

Daarnaast heeft Khonraad in haar systeem maatregelen getroffen om te waarborgen dat de gegevensverwerking veilig en integer is:

- Khonraad is ISO/IEC 75001:2013 gecertificeerd, NEN 7510-1:2017 gecertificeerd en heeft een ISMS ingericht[18]
- Toegang tot het Khonraad-systeem verloopt via twee factor authenticatie (via sms)
- Alle gebruik van het Khonraad-systeem wordt in het systeem gelogd
- Na uitvoeren van een taak in het systeem (bijvoorbeeld registratie van een melding, of de beslissing crisismaatregel door de burgemeester) kan de informatie in Khonraad-systeem niet meer veranderd worden.

[16] zie: https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/
[17] Zie: https://wetten.overheid.nl/BWBR0042237/2019-05-23
[18] Een kopie van het ISO 75001 certificaat, het NEN 7510 certificaat, de Verklaring van Toepasselijkheid (VVT) en de ISMS-risicobeoordeling zijn op aanvraag bij de firma Khonraad beschikbaar.

8 (AVG-)rechten van betrokkenen (art. 12 – 23 AVG)

8.1 Informeren van betrokkene

Het recht op inzage, op grond van de AVG (art. 12 lid 1 AVG) is in de Wvggz van toepassing.

In de praktijk is het recht op toegang waarschijnlijk beperkt, omdat art. 13 lid 4 AVG en art. 14 lid 5 sub a AVG van toepassing zijn: de verwerkersverantwoordelijke hoeft niet te voldoen aan een informatieverzoek als betrokkene reeds over de gevraagde informatie beschikt.

In de praktijk zal een informatieverzoek op grond van de AVG daarom weinig toevoegen, en weinig nieuw informatie opleveren, omdat alle informatie rondom melding, verkennend onderzoek, medische verklaring, crisismaatregel en zorgmachtiging als onderdeel van het dossier al met de betrokkene (en zijn advocaat) is gedeeld.

Om het recht op informatie verder te kunnen borgen is opnieuw het belang van de gestandaardiseerde informatieproducten groot: op die manier weet betrokkene welke informatieproducten (en welke informatie in die producten) beschikbaar zijn.

In de Wvggz zijn diverse momenten dat de gemeente informatie verstrekt aan anderen, of informatie ontvangt van anderen. Betrokkene heeft het recht om te weten welke gegevens aan welke partijen zijn verstrekt. De overdrachten van gegevens zijn in de Wvggz in detail gespecificeerd, en in de bijlage bij deze DPIA in detail beschreven.

Andere overdrachten, dan die in de Wvggz wettelijk zijn voorgeschreven zijn op grond van art. 8:34 Wvggz (algemene geheimhoudingsplicht) door de burgemeester of het college van B&W niet toegestaan.

8.2 Gebruik van toestemming

Zie paragraaf 6.2 voor een toelichting op het gebruik van toestemming in de uitvoering van de Wvggz.

8.3 Recht overdraagbaarheid

Dit recht op overdraagbaarheid is in de Wvggz niet van toepassing, omdat niet is voldaan aan de vereisten in art. 20 lid 1 AVG.

8.4 Recht op rectificatie en verwijdering

Zie de toelichting in paragraaf 6.2. voor een toelichting op het gebruik van 'toestemming'.

De Wvggz biedt diverse manieren waarop betrokkene zijn rechten kan doen gelden, maar gezien de aard van de zorg (namelijk: verplicht) zijn de rechten van betrokkene om gegevens te mogen rectificeren of verwijderen wel beperkt.

Omdat alle gegevens die in de Wvggz worden verwerkt een duidelijk omschreven doel hebben en een duidelijke grondslag, zal er in de praktijk geen sprake zijn van een recht op verwijdering van persoonsgegevens.

Waar de gemeente gegevens onrechtmatig heeft verwerkt (d.w.z. niet op basis van een grondslag in de WVggz), is er uiteraard wel een grond voor een verzoek tot verwijdering. Betrokkene kan daartoe een verzoek doen bij de gemeente, op grond van de AVG. Ook kan betrokkene op grond van de Wvggz in bezwaar geen tegen de opgelegde verplichte zorg, en in die procedure eisen dan de onrechtmatig geregistreerde gegevens worden herzien, c.q. verwijderd.

8.5 Recht op beperken van de verwerking en recht op bezwaar

Zie de toelichting hierboven in paragraaf 8.4 bij het recht op rectificatie en verwijdering.

8.6 Verplichtingen van verwerkers

De verwerkingsverplichting zijn in de Wvggz in detail en specifiek beschreven, evenals de mogelijkheden / verplichtingen om gegevens met andere partijen te delen. Zie hiervoor de bijlage.

Zie verder de toelicht in paragraaf 3.1 t/m 3.4.

8.7 Gegevensoverdracht buiten de Europese Unie

Zie paragraaf 3.5.

9 Risico's bij de gegevensbewerking

De AVG stelt dat de verwerkingsverantwoordelijke een inschatting moet maken van de risico's die verbonden zijn aan de verwerking van de persoonsgegevens. Risico's kunnen nadeel opleveren voor de betrokkenen, maar het kan ook gaan om risico's voor de gemeente, of de gemeentelijke organisatie.

De AVG stelt (art. 35 lid 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 natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens."

In dit hoofdstukken worden de risico's geanalyseerd, die de gemeente loopt in de verwerking van persoonsgegevens bij de uitvoering van de Wvggz. In het volgende hoofdstuk zijn maatregelen geformuleerd ter voorkoming van de risico's of ter mitigatie van de gevolgen.

9.1 Risico-bronnen

9.1.1 Risico's als gevolg van onvoldoende technische beveiligingsmaatregelen

Risico 1.1. Tekortkomingen in de technische beveiliging van systemen

Als de informatiesystemen, waarmee de persoonsgegevens worden verwerkt onvoldoende zijn beveiligd kan dit (onder andere) de volgende nadelen tot gevolg hebben:

- gegevens kunnen in handen komen van ongeautoriseerde personen, of zelf in het openbaar
- de integriteit en juistheid van de gegevens kan niet worden gewaarborgd
- gegevens kunnen onrechtmatig of ongecontroleerd worden verwijderd, of er kan onjuiste informatie aan dossiers worden toegevoegd

Risico 1.2. Tekortkomingen in de (technische) toegang tot gegevens

Het is van belang dat de toegang tot de gegevens goed is beveiligd, en dat alleen geautoriseerde personen, met de juiste rollen en verwerkingsmogelijkheden toegang tot de gegevens en de functionaliteiten in de systemen hebben. Ook het kan het gevolg zijn:

- gegevens in de handen van ongeautoriseerde personen
- de integriteit, juistheid en volledigheid van de gegevens is niet geborgd

9.1.2 Risico's m.b.t. de juistheid en proportionaliteit van de persoonsgegevens

Risico 2.1. Risico dat teveel gegevens worden verzameld

De Wvggz beschrijft in detail welke persoonsgegevens, door welke organisaties / ketenpartners gebruikt mogen worden om tot een besluit of een processtap in de uitvoering van de Wmo te

komen. In aanvulling daarop zijn gestandaardiseerde informatieproducten afgesproken, om te borgen dat de verzamelde persoonsgegevens proportioneel zijn en relevant voor de taakuitoefening.

Het risico dat de gemeente teveel gegevens verwerkt / verzamelt in de Wvggz kan met ontstaan bij:

- Uitvoering van het verkennend onderzoek, als de gemeente teveel informatie over betrokkene en de context van de melding opvraagt bij andere partijen
- In de beslissing van de crisismaatregel, als de burgemeester meer informatie vraagt dan in de gestandaardiseerde informatieproducten is afgesproken (N.B. als de burgemeester de noodzaak van extra gegevens, aanvullend op de gestandaardiseerde informatieproducten kan onderbouwen, is levering van meer gegevens rechtmatig, en toegestaan. Het kan bijvoorbeeld zijn dat de burgemeester met de psychiater wil overleggen. Gezien de ernst van de beslissing voor een crisismaatregel is deze zorgvuldigheid terecht. Het is dus niet zo dat het uitvragen van meer informatie over bijvoorbeeld de context verboden is, maar het is wel van belang dat de burgemeester zich bewust is van de risico's en van de noodzaak om alleen relevante informatie te vragen, die proportioneel is ten opzichte van het besluit dat moeten worden genomen)
- In het delen van gegevens met andere partijen buiten de standaard informatieproducten om

Risico 2.2. Risico dat wettelijke termijnen overschreden worden

In de Wvggz zijn diverse behandeltermijnen in detail en specifiek beschreven. De gemeente of de burgemeester heeft in de Wvggz de taak om een deel van die termijnen te bewaken.

Voorbeelden van afgebakende termijnen voor de gemeente in de Wvggz:

- uitvoering van het verkennend onderzoek naar aanleiding van een melding (maximaal 14 dagen)
- verlenen van verplichte zorg voorafgaand aan een crisismaatregel (maximaal 18 uur)
- de uitvoering van de crisismaatregel starten (maximaal binnen 24 uur)
- de duur van de crisismaatregel (maximaal 3 dagen)

Als de gegevens over datum en tijdstip waarop acties zijn gestart niet goed in de systemen zijn geregistreerd, of als – door onvoldoende beveiliging – de integriteit van die tijdstip-gegevens niet kan worden gegarandeerd, dan wordt de bewaking van de termijn problematisch. Ook de verantwoording achteraf (aan betrokkenen, zijn advocaat of aan de rechter bij een beroepsprocedure) over het gehaald hebben van de termijnen wordt dan problematisch.

Risico 2.3. Onjuiste interpretatie van vanuit betrokkene of vanuit ketenpartners verkregen gegevens

In de Wvggz worden diverse gegevens over betrokkene verwerkt, die zijn verkregen op basis van een mening van betrokkene zelf, of een visie of beoordeling door anderen. Voorbeelden van zulke gegevens zijn:

- De informatie in een melding, bevatten een beoordeling van de situatie door de melder
- Bij het horen wordt de visie van betrokkene gevraagd, terwijl onduidelijk kan zijn in hoeverre betrokkene op dat moment een juiste beoordeling van zijn eigen situatie of de omstandigheden kan maken Onjuiste besluiten (crisismaatregel, wel / niet doorzetten zorgmachtiging)
- De beslissing crisismaatregel wordt voornamelijk genomen op basis van de medische verklaring, een beoordeling van de psychiater, die betrokkene heeft onderzocht en geobserveerd

- Bij de vraag of het resultaat van een verkennend onderzoek moet worden doorgezet als een aanvraag voor een zorgmachtiging kan de gemeente een ambtelijk advies laten opstellen. Dat advies is gemaakt door medewerkers van de gemeente, waarbij het van belang is dat alle partijen zich bewust zijn op grond van welke informatie, observaties of afwegingen dat advies is opgesteld.

Risico 2.4. Meldingen Wvggz worden niet op de juiste manier behandeld.

De mogelijkheid tot het doen van een melding is nieuw in de Wvggz, ten opzichte van de BOPZ. Het is een belangrijke toevoeging, omdat het essentiële naasten en andere de mogelijkheid geeft om hun zorgen om een persoon op een eenduidige plek neer te leggen.

Het is wel van belang dat de gemeente meldingen op de juiste manier weegt en beoordeelt:

- Het risico is dat bij een melding teveel wordt gevaren op de (soms eenzijdige) visie van de melder, zonder dat voldoende wordt gepoogd om de feiten (in het verkennend onderzoek) te verifiëren.
- Andersom is het risico dat een melding juist onvoldoende serieus wordt genomen, en essentiële signalen over de noodzaak van (verplichte) zorg voor een persoon worden gemist
- De gemeente moet zorgen dat de drempel om te melden niet te hoog is, maar tegelijkertijd moet zij voorkomen dat mensen te lichte zaken gaan melden. Verplichte zorg is een 'ultimum remedium', en een melding daarover moet een serieuze achtergrond hebben.
- In de praktijk kan zowel voor de melder als voor de gemeente lastig zijn om te zorgen dat eemn melding bij het juiste 'loket' wordt gedaan. De gemeente zal een manier moeten vinden om meldingen Wvggz te laten aansluiten bij – en strikt te onderscheiden van – de mogelijkheden van meldingen bij een Meldpunt Bemoeizorg, een Meldpunt Zorg & Overlast, een veldmelding bij het Zorg- en Veiligheidshuis, of een melding bij Veilig Thuis.

Risico 2.5. Persoonsgegevens vanuit de Wvggz raken vermengd met gegevens voor andere taken

De AVG (en de Wvggz) vereist dat persoonsgegevens alleen gebruikt mogen worden voor een uitdrukkelijk doel waarvoor de gegevens zijn verzameld (art. 5 lid 1 sub b AVG).

De uitvoering van de Wvggz raakt nauw aan de uitvoering van andere taken door de gemeente, en door ketenpartners. Voorbeelden van dergelijke raakvlakken zijn:

- De melding en het verkennend onderzoek zijn in veel gemeenten belegd, bij een partij (bijvoorbeeld de GGD), die ook taken uitvoert in de bemoeizorg, het tegengaan van overlast en de verlening van openbare ggz. De partij moet deze taken goed gescheiden houden van de Wvggz-taken
- De burgemeester heeft een taak bevoegdheid in het bewaken van de openbare orde en veiligheid (art. 172 Gemeentewet). Die taak kan op gespannen voet staan met de uitvoering van de Wvggz. De Wvggz vereist dat voor een crisismaatregel niet alleen het ernstig nadeel moet worden vastgesteld (wat vaak kan worden gerelateerd aan een verstoring van de openbare orde), maar de burgemeester moet ook vaststellen dat het ernstig nadeel het gevolg van is een psychische stoornis, en dat de verplichte ggz-zorg nodig is (en waarschijnlijk effectief is) om het nadeel weg te nemen. Met andere woorden: de burgemeester mag de Wvggz niet 'misbruiken' om zijn taken m.b.t. de handhaving van de openbare orde en veiligheid te doen.

- Een belangrijk doel van de Wvggz is voorkomen van verplichte zorg. Daarvan afgeleid is het doel dat de gemeente zorgt voor toeleiding van betrokkene naar andere (lichtere) vormen van (vrijwillige) zorg, zoals openbare ggz-zorg, wmo-hulpverlening of vormen van bemoeizorg. In de uitvoering van die taken zijn vaak dezelfde partijen betrokken, die ook betrokken zijn bij de Wvggz (ggd, ggz-instellingen, hulpverleners, politie, openbaar ministerie). Alle partijen moeten de scheiding van de persoonsgegevens, die voor de verschillende taken zijn verzameld, goed in het oog houden.

Risico 2.6. Beleidsinformatie / statistiek is naar persoonsgegevens over betrokkenen terug te leiden

Als beleidsinformatie of statistiek terug te leiden is naar personen, dan bestaat het risico dat die persoonsgegevens openbaar worden, met alle risico's vandien voor betrokkene (stigmatisering, imagoschade e.d.). De wet (AVG, Wvggz, CBS-wet) vereist ook dat openbaar gepubliceerde beleidsinformatie of statistiek niet tot personen herleidbaar mag zijn.

9.1.3 Risico's in de organisatie van de uitvoering van de Wvggz en in de gemeentelijk privacy-organisatie

Risico 3.1. Mandatering, delegatie en opdrachtverlening bij de uitvoering door derden is onvoldoende geregeld

De Wvggz regelt een ernstige inbreuk in de vrijheden en rechten van betrokkenen. Onvrijwillige (psychische) zorg is heel ingrijpend en moet zo veel mogelijk voorkomen worden. Het is een ernstige ingreep in de onaantastbaarheid van het lichaam (dit is één van de grondrechten, art. 11 van de Grondwet). De Wvggz borgt daarom dat het besluit tot een crisismaatregel of zorgmachtiging zorgvuldig wordt genomen.

Onderdeel van die zorgvuldige besluitvorming is dat de taken en bevoegdheden in de Wvggz nauwkeurig zijn geregeld. Als de mandatering of bevoegdheidsverlening van taken naar derden niet correct is geregeld, dan is de uitvoering van die taak door die functionaris onrechtmatig, en is de genomen beslissing als gevolg daarvan ook onrechtmatig.

Bijvoorbeeld: als een beslissing tot een crisismaatregel is genomen door een wethouder, die onjuist of onvolledig is gemandateerd om dat besluit te nemen, dan is het besluit onrechtmatig, en kan de advocaat de beslissing tot de crisismaatregel met succes bij de rechter aanvechten.

Een ander voorbeeld is als de bevoegdheidsverlening aan de uitvoerder van het verkennend onderzoek onjuist is geregeld, dan kan dat ertoe leiden dat de informatie, die in het verkennend onderzoek wordt verzameld wordt gezien als onrechtmatig verkregen. Dat kan er toe leiden dat de rechtmatigheid van een verzoek tot voorbereiden van een zorgmachtiging in gevaar komt.

Risico 3.2. Medewerkers zijn zich onvoldoende bewust van privacyrisico's

De meeste inbreuken op de privacy, of datalekken ontstaan door onzorgvuldig of nalatig handelen door medewerkers van de eigen organisatie. In de uitvoering van de Wvggz worden gevoelige

persoonsgegevens verwerkt (o.a. medische gegevens en strafrechtelijke gegevens) over mensen in zeer kwetsbare posities, met beslissing als gevolg, die voor de betrokkenen zeer ingrijpend kunnen zijn.

Het is van het grootste belang dat de medewerkers van de gemeente, en van de organisaties die taken in opdracht van de gemeente uitvoeren zich te volle bewust zijn van deze belangen, en van de noodzaak om zorgvuldig, beveiligd en vertrouwelijk om te gaan met de persoonsgegevens

Risico 3.3. De privacy organisatie van de gemeente schiet tekort

De AVG stelt eisen aan de privacy-organisatie van een verwerkingsverantwoordelijke, zie hoofdstuk IV, art 24 t/m 43 van de AVG. Eisen vanuit de AVG zijn (onder andere!) :

- Invulling geven aan de taken van de verwerkinsverantwoordelijke
- Regelen van afspraken met verwerkers (via een verwerkersovereenkomst)
- Het inrichten van een register van verwerkingen
- Het uitvoeren van DPIA's op de uitvoering
- Het regelen van technische en organisatorische beveiligingsmaatregelen
- Het melden en registreren van datalekken
- Het aanwijzen van een FG er organiseren dat er toezicht is op de gemeentelijke gegevensverwerking
- Het periodiek evalueren (en aanpassen, c.q. verbeteren!) van het gemeentelijk privacy-beleid en de privacy-organisatie

Ter ondersteuning van de privacy-organisatie heeft de gemeente in het algemeen ook één of meer privacy-officers, en information-security officers in dienst, die de organisatie helpen om de noodzakelijke maatregelen ter borging van de gegevensbescherming en informatiebeveiliging te nemen.

Als deze organisatie van gemeentelijke gegevensbescherming en informatiebeveiliging onvoldoende is, dan is er een risico op datalekken, onrechtmatige verwerking van persoonsgegevens, e.d.

Risico 3.4. De gemeentelijke organisatie en de uitvoering van de Wvggz heeft onvoldoende lerend vermogen ten aanzien van privacybescherming en informatiebeveiliging

Een belangrijke eis vanuit de AVG is dat de gemeente leert van fouten of tekortkomingen in de uitvoering van de Wvggz of de AVG.

De AVG stelt (art. 24 lid 1 AVG): "[…] de verwerkingsverantwoordelijke [treft] passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. *Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.*" (onderstreping door de auteur van deze DPIA).

Zowel de AVG als de uitvoering van de Wvggz bieden diverse mogelijkheden om te leren van 'fouten' of onvolkomenheden:

- De AVG vereist een periodieke beoordeling van en verantwoording over de werking van de gemeentelijke privacy-organisatie (art. 5 lid 2 AVG)
- Door datalekken te onderzoeken ontstaat inzicht in waar de organisatie tekort schiet

- In de Wvggz bieden beroepsprocedures of klachten vanuit betrokkenen inzicht in onvolkomenheden in de uitvoering
- Rapporten van de IGJ (over de uitvoering van de Wvggz) of van de AP (over privacy-beleid in relatie tot de Wvggz) geven informatie over punten, die voor gemeenten van belang zijn. Dit kunnen rapporten zijn die over de eigen gemeente gaan, maar ook rapporten van andere gemeenten. Deze rapporten zijn vaak openbaar toegankelijk.
- Bij privacyschendingen, datalekken, of andere issues met de informatiebeveiliging kan de Informatiebeveiligingsdienst (IBD) van de VNG gemeenten helpen en adviseren over het oplossen van de issues en het in de toekomst voorkomen daarvan.

9.2 Gevolgen van de risico's voor betrokkenen

De gevolgen van bovenstaande risico's kunnen ernstig en ingrijpend zijn. Mogelijke gevolgen *voor betrokkene* van het zich voordoen van de risico's omvatten:

- Lichamelijke, materiële of immateriële schade
- Onrechtmatige vrijheidsbeneming, uitsluiting van dienstverlening, gedwongen onjuiste ggz-zorg
- Financiële verliezen voor betrokkene
- Imagoschade of reputatieschade
- Betrokkene wordt verhinderd om rechten en vrijheden uit te oefenen, in het bijzonder:
    - Het (grond) recht op onaantastbaarheid van het lichaam kan onrechtmatig geschonden zijn
    - Betrokkene kan verhinderd worden om de rechten van betrokkenen in het kader van privacywetgeving uit te oefenen (inzagerecht, correctierecht e.d.)
- Het recht op het vertrouwelijk blijven van persoonlijke gegevens kan worden geschonden
- Verlies van vertrouwelijkheid van door een beroepsgeheim beschermde persoonsgegevens. In de Wvggz gaat het dan onder andere ook om medische gegevens en justitiële- en strafvorderlijke gegevens.
- Betrokkene wordt geconfronteerd met (overheids)bemoeienis waar geen of onvoldoende wettelijke basis voor bestaat. Dit kan leiden tot willekeur in overheidshandelen en ontbreken / wegvallen van rechtsbescherming
- Betrokken kan de controle verliezen over het gebruik van (de eigen) persoonsgegevens
- Betrokkene kan geconfronteerd worden met foute (interpretaties van) gegevens, die op onduidelijke of een niet te reconstrueren manier zijn ontstaan, eventueel in combinatie met onterechte omkering van de bewijslast bij het willen corrigeren van deze gegevens
- Doordat de doelbinding niet correct is gevolgd, wordt in andere hulpverlening geconfronteerd met informatie die niet voor die taak is verstrekt, met vooringenomen hulpverleners, of met het ontzeggen van toegang tot de andere hulpverlening op onrechtmatige gronden.

9.3 Gevolgen van de risico's voor de gemeente

De realisatie van de opgesomde risico's hebben niet alleen gevolgen voor betrokkenen. De risico's kunnen ook ingrijpende gevolgen hebben voor de gemeentelijke organisatie (c.q. de functionarissen die de gemeentelijke taken van de Wvggz uitvoeren, inclusief de burgemeester).

Als er sprake is van onrechtmatige verwerking van persoonsgegevens, onvoldoende maatregelen in de bescherming van privacy of tekortkomingen in de informatiebeveiliging kan dit (onder andere) de volgende ingrijpende gevolgen voor de gemeente hebben:

- Het ontstaan van financiële schade, met mogelijk de eis tot schadevergoeding als gevolg

- Boetes op grond van de AVG, of aanwijzingen vanuit de Autoriteit Persoonsgegevens, voor aanpassing van de gemeentelijke privacy-organisatie
- Verscherpt toezicht vanuit de Inspectie Gezondheidszorg en Jeugd, of vanuit de Autoriteit Persoonsgegevens
- Het creëren van rechtsongelijkheid voor inwoners, en daarmee het verzaken van één van de kerntaken van de overheid
- Door het onrechtmatig handelen van de gemeenten verliest betrokkene het vertrouwen in de gemeente / overheid. De kloof tussen burger en overheid wordt vergroot. Dit ontstaan van wantrouwen kan ook doorwerken naar mensen in de omgeving van betrokkenen (“dit kan mij dus ook overkomen”)
- Door het handelen van de gemeente verliest betrokkene het vertrouwen in de hulpverlening en medische zorg
- Agressie vanuit cliënten richting hulpverleners, of richting functionarissen van de gemeente
- Imagoschade voor de gemeente, politieke schade
- Onrechtmatige procesgang, waardoor Wvggz-maatregelen en gemeentelijke beslissingen onrechtmatig blijken
- Door onzorgvuldig handelen ontstaat wantrouwen in de samenwerking tussen de ketenpartners. De effectieve samenwerking tussen de partijen is geschaad.

10 Geplande en bestaande maatregelen

Het doel van een DPIA is om, op grond van de geïnventariseerde risico's te komen tot maatregelen ter voorkoming dat de risico's zich voordoen. De DPIA biedt daarnaast de mogelijkheid om de maatregelen te plannen, en om vervolgens verantwoording over de maatregelen, en de effecten daarvan te kunnen afleggen.

Hier kan (opnieuw) worden verwezen naar Art. 24 lid 1 van de AVG, waarin de taak van de verwerkingsverantwoordelijke is gegeven: "Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, *treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd.* Die maatregelen worden geëvalueerd en indien nodig geactualiseerd." (onderstreping opnieuw door de auteur van deze DPIA.)

In dit hoofdstuk zijn de maatregelen gegeven, die noodzakelijk zijn om de risico's uit het vorige hoofdstuk te voorkomen, of de effecten van die risico's te mitigeren. Bij alle maatregelen is eveneens aangegeven hoe de gemeente aan de maatregel kan voldoen, of hoe de gemeente, als gevolg van de wettelijke verplichtingen, al voldoet aan de maatregelen.

De te treffen maatregelen zijn samen te vatten in **drie vuistregels** voor de gegevensverwerking door gemeenten, in de uitvoering van de Wvggz:

1. Gebruik een informatie-systeem dat voldoet aan de standaard informatieproducten, de wettelijke Wvggz-vereisten voor gegevensverstrekkingen en de gangbare normen voor informatiebeveiliging (in casu: gebruik het Khonraad-systeem in combinatie met een Veilige Mail voorziening conform NTA 7516.)
2. Gebruik het gezond verstand bij het verzamelen, vastleggen of verstrekken van gegevens. Wees je als persoon en als organisatie steeds bewust van de gevoeligheid van de gegevens en het belang van de Wvggz-verwerkingen voor betrokkene (mede gezien de kwetsbare positie waar betrokkene in verkeert).
3. Organiseer het eigen leervermogen. Leer van geconstateerde fouten en tekortkomingen. Doe ervaring op om uit te vinden wat een goede en effectieve werkwijze is voor meldingen en het verkennend onderzoek. Richt voor de Wvggz een uitvoeringsorganisatie, en een samenwerkingscultuur in, waarin fouten veilig (doch vertrouwelijk) gemeld kunnen worden, en er lering uit te kan worden getrokken.

10.1 Technische maatregelen en informatiebeveiliging

Maatregel 1.1. Gebruik gecertificeerde, goed beveiligde informatiesystemen

Er zijn diverse nationale en internationale normen voor ICT-informatiebeveiliging, en voor de inrichting van een goede ICT-security-organisatie. Ook vanuit de Wvggz-wet zijn eisen en richtlijnen af te leiden. In het bijzonder geldt:

- Gebruik een informatiesysteem dat voldoet aan de standaard informatieproducten, zoals opgesteld door het Wvggz Ketenprogramma, en zoals vastgesteld door de (koepels van) de ketenpartners in de uitvoering van de Wvggz.
- Gebruik een informatiesysteem dat voldoet aan de eisen in het document: 'Harmonisatie maatregelen Informatiebeveiliging Wvggz, Programma Wvggz, 15 december 2018, versie 1.0 definitief'.
- Gebruik een informatiesysteem dat voldoet aan alle wettelijke Wvggz-voorschriften voor vertrekking en ontvangst van persoonsgegevens, en dat voldoet aan de in de wet voorgeschreven maatregelen voor 'privacy-by-design'
- Gebruik informatiesystemen die gecertificeerd aantoonbaar voldoen aan de NEN-75001 norm voor informatiebeveiliging en gegevensbescherming
- Gebruik informatiesystemen die voldoen aan de vereisten vanuit de Baseline Informatiebeveiliging Overheid (BIO v1.03)
- Gebruik een Veilige Mailvoorziening die voldoet aan de vereisten vanuit de NTA 7516

Beoordeling van deze maatregel: als de gemeente voor haar taken gebruikt maakt van het Khonraad systeem, in combinatie met een NTA 7516-conforme veilige mailvoorziening, dan is aan deze maatregel voldaan.

Maatregel 1.2. Gebruik beveiligde mail voor overige gegevensdelingen

De gestandaardiseerde en vanuit de wet voorgeschreven informatieproducten kunnen worden gedaan via het primaire processysteem (Khonraad). Voor alle overige vormen van informatiedeling dient een voorziening voor veilige mail te worden gebruikt. Daarbij gelden als voorwaarden:

- Gebruik een mailvoorziening die voldoet aan de NTA 7516 (zoals Zivver of Zorgmail)
- Gebruik voor het verstrekken van persoonsgegevens in de uitvoering van de WVggz alleen de veilige mailvoorzieningen. Gebruik hiervoor nooit een reguliere mailvoorziening. Maak instructies voor de medewerkers over het gebruik van de veilige mail
- Beperkt het gebruik van de veilige mailvoorziening, voor zover de uitvoering van de Wvggz en de noodzaak tot zorgvuldige afweging en informatievergaring dat toelaat.
- Ontwikkel een etiquette voor het gebruik van veilige mail, en instrueer de medewerkers daarover
- Voorkom dat in de header / berichtinformatie van de veilige mail persoonsgegevens zijn getoond. Deze informatie kan namelijk in de reguliere mail getoond, ter alertering van de ontvanger dat er een veilig mailbericht klaarstaat.
- Maak afspraken over het gebruik van functionele mailboxen (in tegenstelling tot aan een persoon gekoppelde mailbox, bijvoorbeeld een mailbox voor de 'hoorfunctie van gemeente X')
- Zorg dat veilige mails, die zijn ontvangen in de uitvoering van de Wvggz kunnen worden onderscheiden van overige veilige mailberichten.

Beoordeling van deze maatregel: Door gebruik van een veilige mailvoorziening (zoals Zivver of Zorgmail) is aan deze voorwaarde voldaan. De instructie van de medewerkers en het maken van afspraken over het gebruik van de mailvoorziening is de verantwoordelijkheid van de individuele gemeenten.

Maatregel 1.3. Regel autorisaties en toegangsbeperking voor medewerkers

Het is van belang dat alle informatiesystemen alleen benaderd kunnen worden, door medewerkers die daartoe geautoriseerd zijn. Dit betekent:

- Regel op de informatiesystemen adequate toegangsbeveiliging, door middel van een password en een twee factor authenticatie
- Regel voor de informatieverwerking via een mobiele telefoon (zoals de beslissing crisismaatregel, die de burgemeester via een mobiele telefoon kan doen) adequate toegangsbeveiliging.
- Zorg dat in het informatiesystemen via rollen en autorisaties is geregeld dat een medewerker alleen toegang heeft tot de informatie, die voor zijn taakuitoefening in de Wvggz relevant is
- Zorg voor regelmatige updates van de besturingssystemen, en dwing het periodiek herzien van passwords voor de toegang af
- Wijs een medewerkers van de gemeente aan die verantwoordelijk is voor het beheer van de inlog-accounts, en de rollen, en die de communicatie met Khonraad doet over het aanmaken of verwijderen van accounts

Beoordeling van deze maatregelen: Door gebruik van het Khonraad-systeem, en een NTA 7516-conforme veilige mailvoorziening is voldaan aan de technische voorwaarden.[19] Het is aan de gemeente om te voorzien in de organisatorische voorwaarden.

10.2 Maatregelen voor het borgen van de juistheid en proportionaliteit van de gegevens

Maatregel 2.1. Volg de gestandaardiseerde informatieproducten

Gebruik van de gestandaardiseerde informatieproducten heeft vanuit privacy-perspectief een aantal belangrijke voordelen:

- De inhoud van de producten is vastgesteld door vertegenwoordigers van alle betrokken ketenpartijen
- De inhoud is getoetst aan de Wvggz-wet en de wettelijke voorschriften voor gegevensdeling. Door de informatieproducten te gebruiken is op voorhand geborgd, dat de gegevensdeling voldoet aan wat wettelijk is toegestaan
- De inhoud van de producten is ontworpen op het principe van data-minimalisatie.
- Door standaardproducten te gebruiken is voor alle betrokkenen voorspelbaar welke informatie verwerkt zal worden. Dit bevordert de transparantie van de gegevensverwerking

Beoordeling van deze maatregel: De informatieproducten zijn voor gemeenten ingebouwd in het Khonraad-systeem. Door gebruik van dat systeem is het juiste gebruik van de informatieproducten geborgd.

[19] Voor het Khonraad-systeem is een autorisatie-matrix beschikbaar. Deze is opvraagbaar bij Khonraad.

Maatregel 2.2.Volg de wettelijke voorschriften voor gegevensverwerking en gegevensdeling

De wetstekst is specifiek over welke gegevens op welke momenten met welke partijen gedeeld mogen (c.q. moeten) worden. Deze gegevensvertrekkingen zijn in de bijlage beschreven. Om te kunnen voldoen aan de AVG-beginselen van rechtmatigheid, behoorlijkheid en transparantie, het beginsel van doelbinding en minimale gegevensverwerking (art. 5 lid 1 AVG), moet worden geborgd in de gegevensverwerking de wettelijke voorschriften strikt gevolgd worden.

Omwille van de dataminimalisatie en de doelbinding is het advies om terughoudend te zijn met het verzamelen of verwerken van gegevens, die niet in de wettelijke voorschriften (c.q. in d beschrijving van de verwerkingen in de bijlage bij deze DPIA) zijn opgenomen,

Beoordeling van deze maatregel: Net als bij de informatieproducten, zijn de wettelijke voorschriften ingebouwd in het Khonraad-systeem. Door gebruik van dit systeem is geborgd dat voldaan is aan de voorschriften.

Maatregel 2.3. Zorg dat wettelijke termijnen bewaakt worden

Het bewaken van de wettelijke termijnen is van belang om de rechtmatigheid van de verplichte zorg te kunnen borgen. Om de termijnen correct te kunnen bewaken is het noodzakelijk dat de startmomenten van de verschillende activiteiten juist en niet-veranderbaar geregistreerd worden. Complicerend kan zijn dat de registratie van een tijdstip soms door de ene partij gebeurt (bijvoorbeeld de start van voorafgaande zorg, door de hulpverlener), terwijl de bewaking van de termijnen door een andere partij gebeurt (bij voorafgaande zorg: de burgemeester). Dit noodzaakt dat partijen in de termijn bewaking de startmomenten, en de deadlines voor activiteiten in hetzelfde systeem registreren, en dat de integriteit van die registratie geborgd is.

Beoordeling van deze maatregel: Ook hier geldt, dat als betrokken partijen samenwerken in het Khonraad-systeem, dat is voldaan aan de vereisten. Als een uitvoerende partij voor bijvoorbeeld het registreren van meldingen of het verkennend onderzoek een ander systeem gebruikt (zoals Clavis of GCOS), dan moeten maatregelen worden genomen om de registratie van de startmomenten en de bewaking van de termijnen goed te borgen.

Maatregel 2.4. Beperk de gegevensuitvraag in het verkennend onderzoek. Doe ervaring op met wat een effectieve werkwijze is voor het verkennend onderzoek

In tegenstelling tot de meeste processen in de Wvggz is de werkwijze voor het verkennend onderzoek in de wet níet in detail en specifiek beschreven. De komende periode zal de gemeente moeten onderzoeken, en ervaren wat voor het verkennend onderzoek een goede werkwijze is. Aan de ene kant moet worden voorkomen dat in het onderzoek teveel (disproportioneel) informatie wordt verwerkt, of dat de doelbinding niet strikt wordt gevolgd. Aan de andere kant moet worden voorkomen dat de inhoud van het verkennend onderzoek zo smal wordt, dat het praktisch altijd zal leiden tot het doorzetten in een zorgmachtiging, en het verkennend onderzoek feitelijk van weinig toegevoegd waarde is, in het voorkomen van verplichte zorg.

Naar de letter van de wet is het doel van het verkennend onderzoek in de wet eng omschreven: het gaat om het vaststellen van (al dan niet) *een vermoeden* van ernstig nadeel, dat vermoedelijk samenhangt met een psychische stoornis, en het nadeel kan vermoedelijk door (onvrijwillige) zorg

worden weggenomen. Dit leidt tot een beperkt verkennend onderzoek, waarin de vermoedens getoetst worden.

Tegelijkertijd is de opdracht van de Wvggz, c.q. het verkennend onderzoek, ook om het ernstig nadeel liefst zonder verplichte zorg terug te dringen, en waar mogelijk verplichte zorg te voorkomen.

De gemeente zal hier een balans moeten vinden tussen enerzijds het uitvoeren van een verkennend onderzoek en het doorzetten van de aanvraag naar een zorgmachtiging, en anderzijds het tijdig doorverwijzen naar andere partijen voor hulpverlening of ondersteuning (zoals Veilig Thuis, bemoeizorg, meldpunt zorg & overlast e.d.).

De taak van de gemeente is om het verkennend onderzoek zo te organiseren dat:

- Omwille van de proportionaliteit en de doelbinding de informatieverzoeken aan andere partijen zoveel mogelijk beperkt blijven
- Voorkomen dat resultaten / inhoud van het verkennend onderzoek voor andere doelen / door niet bevoegde partijen gebruikt worden
- Als de uitvoering verkennend onderzoek belegd is bij een derde partij, moet de gemeente zorgen dat de inhoud / resultaten / uitvoering van het verkennend onderzoek voldoende zijn gescheiden van de reguliere uitvoering van andere taken door de derde partij. Ook de gegevensverwerking voor het verkennend onderzoek moet voldoende gescheiden zijn van de gegevensverwerking voor het verkennend onderzoek.

Beoordeling van deze maatregel: De gemeente zal de komende periode ervaring moeten opdoen met de werkwijze. Vooraf kan (c.q. moet) ingepland worden, dat de werkwijze op enig moment wordt geëvalueerd. De gemeente kan dan beoordelen wat een effectieve manier van werken is voor het verkennend onderzoek. Dit aspect van ‘leren’, ‘evalueren’ en ‘aanpassen’ is toegestaan binnen de AVG en is zelfs een essentieel onderdeel van de privacywetgeving (art. 24 lid 1 AVG)

Maatregel 2.5. Zorg dat Wvggz-meldingen proportioneel en adequaat worden onderzocht.

Een verkennend onderzoek volgt in het algemeen op een Wvggz-melding. De gemeente zal bij meldingen – net als bij het verkennend onderzoek – ervaring moeten opdoen met het juist en effectief ontvangen en verwerken van meldingen. De gemeente moet zorgen dat:

- Meldingen moeten altijd opgevolgd worden
- De privacy van de melder moet worden beschermd, als de melder dat wenst (anoniem melden)
- Feiten en visies in de melding moeten zo goed als mogelijk worden geverifieerd. Hierbij moet de gemeente enerzijds voorkomen dat de melding niet serieus genoeg wordt genomen, maar anderzijds moet ook worden voorkomen dat de (soms gekleurde) visie van de melder te snel als waar wordt aangenomen. In ieder geval moet worden voorkomen dat een betrokkene op grond van een melding op voorhand al gestigmatiseerd wordt.
- In de voorlichting naar het publiek over het meldpunt kan de gemeente sturen in hoe, en in welke situaties meldingen gedaan kunnen worden. De gemeente zal een balans moeten vinden tussen het laag houden van de drempel om te melden, en het voorkomen van ‘onvoldoende serieuze’ meldingen.
- De gemeente moet voorkomen dat de inhoud van melding voor andere doelen gebruikt worden / bij onbevoegde derden terecht komen.

Beoordeling van deze maatregel: Door de registratie van de melding te doen in een passend systeem (dat kan bijvoorbeeld Clavis van de GGD zijn of GCOS van het Zorg- en Veiligheidshuis, of Khonraad) is opvolging van de melding, de bewaking van de termijnen en de scheiding van andere registraties betrekkelijk eenvoudig te organiseren. Voor het vinden van de juiste balans in het omgaan met meldingen zal de gemeente – net als bij het verkennend onderzoek – de komende periode ervaring moeten opdoen. Ook hier geldt: vanuit de privacy-wetgeving is dit toegestaan, mits een evaluatie moment nu al wordt gepland, en de gemeente lering trekt uit de opgedane ervaringen.

Maatregel 2.6. Houdt gegevensverwerking Wvggz gescheiden van de verwerking voor andere taken / wetten

De doelbinding (art. 5 lid sub b AVG) vereist dat gegevens alleen voor de vooraf vastgestelde doelen gebruikt mogen worden. In de uitvoering van de Wvggz betekent dit voor gemeenten:

- Zorg dat de registratie van meldingen Wvggz in de systemen herkenbaar gescheiden is van de registratie van meldingen uit andere wettelijke kaders (zoals Veilig Thuis, veldmelding Zorg- en Veiligheidshuis, Meldpunt Zorg & Overlast e.d.). Voorkom dat onbevoegde personen de Wvggz-meldingen kunnen inzien.
- Zorg dat het verkennend onderzoek in de uitvoering en de registratie voldoende gescheiden is van vergelijkbare onderzoeken bij bijvoorbeeld de GGD (zorg & overlast, bemoeizorg), het Zorg- en Veiligheidshuis (triage en casusoverleg) e.d.
- Voorkom dat de gemeente (of een partij, die in opdracht Wvggz-taken uitvoert) de gegevens die zijn verzameld of verkregen bij een melding, een vekennend onderzoek, een voorbereiding van een zorgmachtiging of een crisismaatregel niet gebruiken voor andere doelen. Gebruik van die gegevens voor die andere taken zonder meer is niet rechtmatig.

Beoordeling van deze maatregel: Het is aan de gemeente (of de uitvoerder) om te organiseren dat de registratie t.b.v. de Wvggz gescheiden van de andere registraties. Dat kan door voor de Wvggz een apart systeem te gebruiken (Khonraad), of door in de gebruikte systemen, door middel van rollen en autorisaties de Wvggz-gegevens af te schermen.

Maatregel 2.7. Wees terughoudend met informatiedeling buiten de wettelijke voorschriften

Veruit de meeste noodzakelijke gegevensverstrekking zijn in de Wvggz expliciet benoemd en uitgewerkt. Zie ook de uitwerking in de bijlage bij deze DPIA. De basisregel in de verwerking van gegevens binnen de Wvggz is: “wat noodzakelijk is, is in de wet beschreven. Als het niet in de wet is beschreven is het waarschijnlijk niet noodzakelijk”.

Als andere gegevens uitgewisseld moeten worden, dan moet daarvoor de beveiligde mail voorziening worden gebruikt.

Overigens heeft de wet expliciet de mogelijkheid van ‘onvoorziene’ gegevensverstrekking ingebouwd: in art. 8:29 Wvggz is een vangnet geregeld, zodat de burgemeester, de politie, de geneesheer-directeur, de zorgverlener en de officier van justitie alle informatie mogen uitwisseling die voor de uitvoering van de wet noodzakelijk is, en die daarnaast noodzakelijk is om het ernstig nadeel terug te dringen. Het feit dat dit ‘vangnet-artikel voor de gegevensverwerking’ er is in de wet, betekent dat het ook gebruikt mag en kan worden.

Beoordeling van deze maatregel: Door de verwerking van de gestandaardiseerde informatieproducten in Khonraad te doen, en voor de overige (zo veel mogelijk beperkte) gegevensvertrekking de veilige mail te gebruiken, kan de gemeente relatief eenvoudig aan deze voorwaarde voldoen.

Maatregel 2.8. Verwerk alleen geanonimiseerde gegevens voor beleidsinformatie en statistiek

De gemeente moet waarborgen dat stuurinformatie, beleidsinformatie en statistiek niet tot een persoon herleid is. Zeker als de beleidsinformatie of statistiek openbaar gedeeld wordt, is deze voorwaarde essentieel.

Beoordeling van deze maatregel: Door gebruik te maken van de rapportagemodules in de beschikbare systemen kan de gemeente relatief eenvoudig aan deze voorwaarde voldoen.

10.3 Organisatorische maatregelen

Maatregel 3.1. Organiseer training en bewustwordingsactiviteiten voor medewerkers

Privacybescherming en het vertrouwelijk omgaan met gegevens van betrokkenen is in belangrijke mate ook een cultuur-aspect van de organisatie. Het is van belang dat medewerkers zich bewust zijn van het belang van de privacybescherming, en zich bewust zijn van de risico's die voort kunnen vloeien uit een slordige omgang met persoonsgegevens. Juist omdat het in de Wvggz gaat om zeer gevoelige informatie, over mensen in uiterst kwetsbare posities, waarbij de zorg niet vrijwillig is, maakt dat dit bewustzijn extra sterk moet zijn.

De gemeente moet zorgen voor:

- Training voor de medewerkers over de privacy-aspecten van de Wvggz
- Bewustwording bij de medewerkers voor het belang van privacybescherming
- Het maken van afspraken met ketenpartners over de uitvoering van de Wvggz-taken en de samenwerking daarin
- Afspraken met aanpalende vormen van zorg en dienstverlening (zoals de bemoeizorg, Veilig Thuis of het Zorg- en Veiligheidshuis) over de eventuele aansluiting tussen de dienstverlening door die partijen, en de uitvoering van de Wvggz

Beoordeling van deze maatregel: Voldoen aan deze maatregel past binnen de reguliere werkwijzen van de gemeente en haar ketenpartners. De gemeentelijke medewerkers, die betrokken zijn bij de uitvoering van de Wvggz en bij de aanpalende dienstverlening, zijn opgeleid in dit domein, en hebben als het goed is nu al dagelijks te maken met cliënten in kwetsbare posities. Bij de training en de bewustwording kan de reguliere privacy-organisatie binnen de gemeente helpen (de FG, de privacy-officer e.d.), of kan de gemeente externe ondersteuning door een privacyexpert vragen.

Maatregel 3.2. Richt de gemeentelijke organisatie in op een veilige gegevensverwerking

De AVG geeft diverse adviezen of voorschriften voor de inrichting van een goede privacy-organisatie. Maatregelen zijn onder andere:

- Voldoe voor de Wvggz aan de wettelijke vereisten vanuit de AVG (uitvoeren DPIA, melden datalekken, aanpassen register van verwerkingen, betrek de FG e.d.) Volg de organisatorische maatregelen uit de Baseline Informatiebeveiliging (BIO v1.03)
- Richt procedures in voor datalekken, melding incidenten informatiebeveiliging en organiseer de opvolging daarvan
- Sluit voor de uitvoering van de Wvggz aan bij de in de gemeente gangbare werkwijze vanuit de privacy- en ICT-security. (Gebruik van een ISMS, inzet van de privacy-officer, rol van de FG e.d.)

Beoordeling van deze maatregel: voldoen aan deze maatregel behoort tot de regulier opdracht van de privacy-organisatie binnen de gemeente. De FG, de privacy officer en de ICT-security-officer van de gemeente beschikken over de benodigde kennis en kunnen hierover adviseren.

Maatregel 3.3. Regel de mandatering, delegatie, opdrachtverstrekking bij uitvoering door derden goed

In de uitvoering van de WVggz kunnen de burgemeester of de gemeente op diverse onderdelen taken delegeren of overdragen aan anderen. Voor de juistheid en rechtmatigheid van de gegevensverwerking die bij die taken hoort, is het noodzakelijk, dat de bevoegdheidsverlening goed georganiseerd is. Zonder een goede bevoegdheidsverlening is de gegevensverwerking onrechtmatig, en is een bestuurlijke beslissing (bijvoorbeeld bij een crisismaatregel) ook onrechtmatig. Het is dus van het grootste belang, dat dit goed geregeld is.

De gemeente moet zorgen dat:

- De beslissing crisismaatregel correct is gemandateerd aan de wethouder(s)
- Dat, in geval van een crisismaatregel, voor alle betrokkenen (zoals ketenpartners, maar ook voor de meldkamer of de crisisdienst) duidelijk is wie op dat moment het bevoegd gezag heeft
- Dat de uitvoering van de melding, het verkennend onderzoek, en het horen van betrokkene – indien aan de orde – op de juiste manier is overgedragen naar / opgedragen aan de uitvoerende partij
- Dat de eventuele ambtelijke voorbereiding van een crisismaatregel correct is gemandateerd

Beoordeling van deze maatregel: als het goed is, heeft de gemeente deze bevoegdheidsverleningen al afgerond voor de invoering van de Wvggz.

Maatregel 3.4. Organiseer periodiek evaluaties

'Leren van fouten' is een belangrijk onderdeel van de continue verbetering, die hoort bij een goed privacybeleid. In de uitvoering van de Wvggz zijn diverse momenten waarop de gemeente kan evalueren, en leren of op de juiste manier met de vertrouwelijkheid van persoonsgegevens is omgegaan:

- Meldt datalekken, en evalueer hoe de beveiliging verbeterd kan worden
- Ga na of in beroepsprocedures ook aspecten van de gegevensverwerking zijn opgenomen. Leer van deze situaties. Hetzelfde geldt voor klachten vanuit betrokkenen (die weliswaar minder ingrijpend zijn dan beroepsprocedures, maar net zo leerzaam kunnen zijn)

- Bekijk onderzoeken vanuit de Inspectie Gezondheidszorg en Jeugd, en de Autoriteit Persoonsgegevens. Dat kunnen rapporten over uw eigen gemeente zijn, maar ook over andere gemeenten
- Organiseer periodiek overleg met de ketenpartners over privacybescherming en informatiebeveiliging.

N.B. Maak van privacybescherming ook een bestuurlijk punt, bijvoorbeeld door het met enige regelmaat te agenderen in het periodiek regionaal bestuurlijk overleg tussen de gemeenten, politie, officier van justitie en de geneesheer-directeuren (art. 8:31 Wvggz). Het regionaal overleg kan worden gebruikt om ervaringen met de privacybescherming te evalueren, om afspraken te maken over zorgvuldig omgaan met persoonsgegevens, en om te bouwen aan vertrouwen in de samenwerking – wat juist voor de privacybescherming zo essentieel is.

Beoordeling van deze maatregel: voldoen aan deze maatregel behoort tot de regulier opdracht van de privacy-organisatie binnen de gemeente. De FG, de privacy officer en de ICT-security-officer van de gemeente beschikken over de benodigde kennis en kunnen hierover adviseren.
Het agenderen van de privacy-ervaringen in het regionaal bestuurlijk overleg kan eenvoudig door de secretaris van dit overleg, in samenwerking met de FG of de privacy-officer van de gemeente(n) gedaan worden.