PBLQ

Privacy in het sociaal domein

Rapportage Rekenkamercommissie Gooise Meren
5977
0.1
12 oktober 2017

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

Overheden beheren veel persoonsgegevens van burgers. Dat geldt bij uitstek voor gemeenten. Daar vindt de registratie in het bevolkingsregister plaats, melden inwoners zich voor een vergunning, voor een uitkering of voor vragen naar zorg of ondersteuning.
Na de decentralisatie moeten meer burgers met een hulpvraag zich wenden tot de gemeente. In de meeste gevallen gaat het om mensen in een kwetsbare positie, die afhankelijk zijn van de ondersteuning door de gemeente. Daarmee is het gegevensverkeer binnen de gemeente complexer geworden: meer cliënten, meer gevoelige gegevens, zoals die over gezondheid, inkomen, justitiecontacten, verhoudingen binnen een gezin en dergelijke. Het betreft bovendien gegevens die gedeeld moeten worden met veel meer externe partijen zoals zorgaanbieders.

Burgers moeten ervan uit kunnen gaan dat hun gegevens bij de gemeente in veilige handen zijn. Gemeenten moeten dat kunnen aantonen. Bescherming van persoonsgegevens is immers een grondrecht.
Wordt dit recht, en daarmee het vertrouwen in de overheid, geschaad, dan kan dat ernstige gevolgen hebben voor de relatie tussen gemeente en burger.

Daarnaast moeten gemeenten er rekening mee houden dat de regelgeving over het beschermen van persoonsgegevens is aangescherpt. De gemeente loopt een risico op hoge boetes als zij niet conform de geldende normen de beveiliging van persoon sgegevens op orde heeft. Het belang van een adequaat privacybeleid en van een strikte uitvoering is daarmee toegenomen.

Uit landelijk onderzoek van de Autoriteit Persoonsgegevens[1] blijkt dat gemeenten over het algemeen nog worstelen met vraagstukken rondom privacy in het sociaal domein. Wat kan en mag? En hoe past dat bij de werkwijze die ze hanteren?

Tegen deze achtergrond heeft de rekenkamercommissie van de gemeente Gooise Meren PBLQ en het bureau Y. Bommeljé Advies en Onderzoek ondersteuning gevraagd bij een onderzoek naar de wijze waarop deze gemeente uitvoering geeft aan de bescherming van persoonsgegevens in het sociaal domein.

Het onderzoek biedt inzicht in het gemeentelijk privacybeleid. In het bijzonder is aandacht besteed aan de wijze waarop in de dagelijkse uitvoeringspraktijk wordt omgegaan met persoonsgegevens.

[1] Autoriteit Persoonsgegevens: Verwerking van persoonsgegevens in het sociaal domein: de rol van toestemming, april 2016.

Juist in de praktijk blijkt of de verplichting om correct om te gaan met vertrouwelijke gegevens breder wordt opgevat dan louter een technisch of juridisch probleem. In de opvatting van de rekenkamercommissie is privacy onderdeel van transparant en professioneel handelen en dat vereist dat je als professional ziet wat de betekenis daarvan is voor de burger. Daarnaast richt het onderzoek zich op de wijze waarop de gemeente aandacht besteedt aan de positie van de burger. Als laatste is ook aandacht besteed aan de rol van de gemeenteraad in het privacybeleid.

De Rekenkamercommissie is zich ervan bewust dat de gemeente Gooise Meren nog jong is en de organisatie zich nog ontwikkelt. Eerder voerde gemeente Bussum ook de taken in het sociaal domein uit voor de gemeenten Naarden en Muiden. Dit gebeurde onder de naam 'Wijzer'. Met de fusie tot Gooise Meren per 1 januari 2016 is Wijzer ingepast in de gemeentelijke organisatie onder de naam Uitvoeringsdienst Sociaal Domein (USD). De huidige organisatieontwikkeling biedt een goede kans om privacy werkende weg in te bedden in de nieuwe organisatie en parallel daaraan privacybewustzijn op de agenda van de medewerkers te houden.

1.2 Opdrachtformulering

Het doel van het onderzoek luidt:

> ***De rekenkamercommissie wil inzicht bieden in het gemeentelijk beleid en de uitvoering rond privacy in het sociaal domein. Het gaat met name om de manier waarop het beleid wordt uitgevoerd en hoe de organisatie en de medewerkers het privacybewustzijn onderdeel maken van hun dagelijkse routine.***

De centrale probleemstelling van het onderzoek is als volgt geformuleerd:

> ***In hoeverre gaat de gemeente Gooise Meren in de dagelijkse praktijk correct om met de persoonlijke gegevens van burgers in het sociale domein?***

Deze hoofdvraag is uitgesplitst in de volgende deelvragen over de onderwerpen beleid, leren en verbeteren, de positie van de burger en de kaderstellende en controlerende taak van de gemeenteraad.

Beleid

1. Wat zijn de gemeentelijke beleidskaders rondom privacy en informatieveiligheid in het sociaal domein? Hoe wordt er geanticipeerd op de AVG? In hoeverre voldoet het beleid aan de wettelijke grondslagen?
2. Hoe is het beleid uitgewerkt en geborgd in processen?
3. Hoe is de toegang tot dossiers (autorisaties) geregeld?
4. Hoe ziet het toezicht op de omgang met de persoonsgegevens er uit?
5. Hoe gaat het in de praktijk, op de werkvloer?
6. In hoeverre voldoet de uitvoering aan de wettelijke normen en de onder 1 genoemde wettelijke kaders?
7. In hoeverre heeft de gemeente een balans gevonden tussen regels en procedures rondom de bescherming van privacy enerzijds en een goede dienstverlening aan de burger anderzijds waarbij zij de hulp krijgen die nodig is?

Leren en verbeteren

8. Op welke manier worden medewerkers betrokken bij, en getraind in het borgen van de privacy en het versterken van de informatieveiligheid?
9. Op welke manier heeft de gemeente het proces van evalueren en verbeteren ingericht?

10. Is er al een evaluatie geweest en hoeverre heeft dat tot verbeteringen geleid?

Positie burger
11. Wanneer en op welke manier geven burgers toestemming voor het gebruik en verwerken van gegevens?
12. Op welke manier worden burgers geïnformeerd over het gebruik en de verwerking van hun persoonsgegevens?

Kaderstellende en controlerende taak gemeenteraad
13. Op welke manier kan de gemeenteraad het beleid rondom privacy en informatieveiligheid in het sociaal domein controleren en sturen?
14. Op welke wijze is de raad tot nu toe betrokken geweest?
15. Is er in het privacybeleid van de gemeente aandacht voor welke acties ondernomen moeten worden in het geval zich een datalek voordoet?

Het onderzoek richt zich op privacy (bescherming persoonsgegevens) en het beleid rond informatiebeveiliging. Bescherming van persoonsgegevens en informatiebeveiliging worden vaak als synoniemen beschouwd maar zijn twee verschillende aspecten. Bij bescherming van persoonsgegevens gaat het om de toepassing van regels die bepalen hoe persoonsgegevens mogen worden verzameld en gebruikt. Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket maatregelen om de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van de gegevens in de organisatie te waarborgen. Het accent van het dit onderzoek ligt op privacy, de wijze waarop uitvoerders met persoonsgegevens omgaan.

1.3 Werkwijze

Bij het uitvoeren van het onderzoek zijn de eerste vier stappen in de periode van april tot en met juli 2017 doorlopen. De laatste stap, het ambtelijk wederhoor en de bestuurlijke reactie hebben plaatsgevonden in september 2017.

1. Documentenstudie
Allereerst zijn gemeentelijke documenten over de inrichting en uitvoering van het privacybeleid verzameld en bestudeerd (zie bijlage).

2. Interviews
Vervolgens zijn verschillende functionarissen geïnterviewd die werkzaam zijn in het sociaal domein en die zich bezighouden met privacy- en beveiligingsbeleid. Daarnaast zijn gesprekken gevoerd met medewerkers inkoop- en contractmanagement en juridische zaken van de Regio Gooi en Vechtstreek (RGV). De RGV voert namelijk het inkoopbeleid en contractmanagement uit voor alle gemeenten in de regio. De medewerker juridische zaken van de RGV heeft bij de opzet van het privacybeleid bij de decentralisaties voor de betrokken gemeenten een belangrijke rol gespeeld. Ook is met de voormalig beleidsmedewerker van het regionale programma Samenkracht! gesproken: een programma waarin burgers en ambtenaren elkaar ontmoeten en specifieke thema's bespreken, waaronder privacy.
Om de ervaringskant van 'de cliënt' te belichten, is gesproken met vertegenwoordigers van de Adviesraad Wmo/Jeugd en van de Adviesraad Werk en Inkomen. Ten slotte zijn met twee zorgaanbieders gesprekken gevoerd. Van alle gesprekken is een verslag opgesteld dat ter toetsing is voorgelegd aan de gesprekspartner.
Een lijst met geïnterviewde functionarissen is opgenomen in de bijlage.

3. Verificatiesessie
Gedurende het onderzoek zijn volgtijdelijk meningen en ervaringen van betrokkenen geïnventariseerd. Daaruit hebben de onderzoekers zich een beeld kunnen vormen over het privacybeleid en hoe daar uitvoering aan wordt gegeven. Dat beeld was niet altijd eenduidig doordat ervaringen en opvattingen van betrokkenen van elkaar kunnen verschillen. Om dat beeld scherper te stellen is een verificatiesessie gehouden. Hiervoor zijn de gemeentelijk medewerkers uitgenodigd die zijn geïnterviewd. In deze sessie zijn de voorlopige bevindingen gepresenteerd en bediscussieerd. Op die manier was het mogelijk om de bevindingen te toetsen, te verdiepen aan te scherpen of te nuanceren.

4. Opstellen rapportage
Ten slotte is aan de hand van de verzamelde informatie het rapport opgesteld met de beantwoording van de onderzoeksvragen. Vervolgens zijn de bevindingen getoetst aan het normenkader dat de Rekenkamercommissie van tevoren had vastgesteld.

5. Ambtelijk wederhoor en bestuurlijke reactie
Conform de overeengekomen procedures is de ambtelijke organisatie de gelegenheid geboden om het ‘feitenrapport’ van commentaar te voorzien. Vervolgens heeft het College van B&W ook bestuurlijk commentaar gegeven op het rapport, inclusief de conclusies en aanbevelingen. Deze reactie is binnengekomen op 10 oktober 2017.

1.4 Indeling rapport

In hoofdstuk 2 komen achtereenvolgens de onderwerpen van het onderzoek aan de orde: het beleid, leren en verbeteren, de positie van de burger en de rol van de raad. Per onderwerp worden de bevindingen gepresenteerd en de deelvragen beantwoord. In hoofdstuk 3 worden de bevindingen aan de hand van het normenkader getoetst. Hoofdstuk 4 bevat de conclusies en aanbevelingen.
In het rapport wordt geregeld verwezen naar organisatieonderdelen en diverse regelingen. Deze worden meestal met hun afkorting aangeduid. Een lijst met gebruikte afkortingen is in bijlage A. opgenomen. De overige bijlagen betreffen overzichten van bestudeerde documenten en de geïnterviewde personen.
In onderzoeken van rekenkamers is het gebruikelijk om met een normenkader te werken dat dienst doet om te bevindingen mee te waarderen. De gehanteerde normen zijn gekoppeld aan de gestelde onderzoeksvragen. Dit normenkader en de verbinding met de diverse onderzoeksvragen is eveneens in de bijlage opgenomen.
Als laatste bijlage zijn ter informatie het vigerende privacyprotocol van de gemeente Gooise Meren opgenomen en de aan alle medewerkers verstrekte ‘Gouden regels’ voor de invulling van privacy in de dagelijkse praktijk.

2. Beantwoording van de onderzoeksvragen

In dit hoofdstuk worden de onderzoeksvragen beantwoord over de onderwerpen: beleid, leren en verbeteren, positie burger en de rol van de raad. Per onderwerp wordt eerst een schets gegeven van de context en de algemene bevindingen zoals die uit het onderzoek naar voren zijn gekomen.

2.1 Algemene bevinding

Uit het onderzoek is duidelijk geworden dat de gemeente Gooise Meren informatiebeveiliging en het beschermen van de privacy van de inwoners voortvarend ter hand heeft genomen. Het beleid doet recht aan wettelijke eisen en richtlijnen.

Het beleid doet recht aan wettelijke eisen en richtlijnen.
Medewerkers van de gemeente zijn bekend met de regels en zeggen daar naar te handelen

Ook de verdere uitwerking van dit beleid krijgt de aandacht. Zo wordt gewerkt aan het afronden van een Evaluatie- en verbeterplan en het opstellen van een nieuw Informatiebeveiligingsplan.

Er is een privacyprotocol en medewerkers van de gemeente zijn bekend met de regels en zeggen daar naar te handelen. Kwaliteitsmedewerkers binnen het sociaal domein letten er op dat medewerkers niet meer informatie in een dossier opnemen dan strikt noodzakelijk is voor de dienstverlening. Ook heeft de gemeente er voor gezorgd dat de persoonlijke gegevens van inwoners alleen toegankelijk zijn voor medewerkers die deze informatie nodig hebben om hun werk uit te voeren. De procedures voor deze autorisaties zijn op orde. Met gebruikmaking van diverse (SUWI- en kwaliteits-)controles komen mogelijke tekortkomingen in het privacybeleid in beeld. Waar nodig wordt actie ondernomen.

Het onderzoek heeft ook een aantal verbeterpunten in beeld gebracht. Vertegenwoordigers van cliëntenorganisaties hebben vragen én zorgen bij het privacybeleid. Vooralsnog worden zij in dit verband te weinig gerustgesteld door het beleid en de voorlichting daarover.

Hoewel er kwaliteitscontroles plaatsvinden, worden het privacybeleid en de uitvoering daarvan niet structureel geëvalueerd en wordt daarover geen verantwoording afgelegd aan de gemeenteraad

2.2 Beleid

Context en bevindingen
De gemeente Gooise Meren is een fusiegemeente die op 1 januari 2016 is ontstaan. De interne organisatie is nog in ontwikkeling. De afdeling Wijzer van de gemeente Bussum is integraal ingepast in de fusiegemeente. Daarmee moest ook het informatiebeveiligings- en privacybeleid sociaal domein

worden ingepast in het privacy- en beveiligingsbeleid van Gooise Meren. Dit beleid is eind 2016 opgesteld.[2]
Eveneens moesten nieuwe werkrelaties tussen de USD en gerelateerde afdelingen worden ingericht, zoals de verbinding met de concern controller en met de chief information security officers (CISO's). Dit inpassingsproces is nog gaande. Vooralsnog wordt zoveel als mogelijk het 'oude' informatiebeveiligingsbeleid van de USD werkende weg vernieuwd. Dat geldt overigens ook voor het gemeentelijk informatiebeveiligingsbeleid, dat na de fusie opnieuw opgezet moest worden. Daarvoor heeft de gemeente extra formatie uitgetrokken in de vorm van twee CISO's, die bezig zijn de informatiebeveiliging te laten voldoen aan alle normen van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Algemene Verordening Gegevensbescherming (AVG). Deze verordening zal op basis van Europese afspraken op 25 mei 2018 moeten worden toegepast.

Aan de vooravond van de decentralisaties in het sociaal domein hebben de gemeenten in de regio Gooi en Vechtstreek (RGV) samengewerkt bij het opstellen van het inkoopbeleid, het beleid voor de Jeugdwet en ook voor het privacybeleid. Aan privacy is toen veel aandacht besteed, vooral omdat dat vanuit de (nieuwe) Jeugdwet wordt vereist.

De RGV is ook beheerder van de infrastructuur voor het uitwisselen van berichten met zorgaanbieders, het Digitaal Leefplein. Na het bepalen van de maatwerkvoorziening voeren de consulenten de gegevens in via het Digitaal Leefplein. Vervolgens worden vanuit de Regio de berichten aan de zorgaanbieders verstuurd en van zorgaanbieders ontvangen. De Regio heeft een stringent beveiligingsbeleid voor deze gegevensuitwisseling ontwikkeld, waarop ook intensief toezicht wordt gehouden. Het (uitvoerings)beleid is pas twee jaar terug ontwikkeld, in de vorm van informatiebeveiligingsbeleid, een privacyprotocol, en verbeterd SUWI-beheer. Dat vormt samen met de bepalingen van de Wbp en de materiewetten de basis voor het handelen.

Vraag 1.1 Wat zijn de gemeentelijke beleidskaders rondom privacy en informatieveiligheid in het sociaal domein?
Het algemene privacykader voor de gemeente vindt vanzelfsprekend zijn basis in de Wbp. De wet bevat algemene normen, die samen een afwegingskader geven. Aan de hand van dat wettelijke afwegingskader moet een gemeente (of bedrijf, instelling) steeds zelf bepalen of een bepaalde verwerking van persoonsgegevens is toegestaan, en zo ja, onder welke voorwaarden.

In gemeentelijke beleidsstukken komt het onderwerp privacy op meerdere plekken aan de orde.

In het *Beleidsplan Sociaal Domein 2015-2018* komt privacy zijdelings aan de orde. Er wordt aangegeven dat privacy een belangrijk aspect is bij de ondersteuning aan burgers en dat er geen informatie wordt gedeeld tussen organisaties zonder de toestemming van de burger. Ook komt in dit beleidsplan het perspectief van inwoners aan de orde: zij willen bescherming van hun privacy, inzage- en correctierecht. Zij willen weten hoe de beveiliging geregeld is en wie toegang heeft tot een dossier. Ook vragen ze om een waarborg dat er privacy mogelijk is op de fysieke plek waar gesprekken worden gevoerd.

In de subnota *Gemeentelijke Dienstverlening* (horend bij het Beleidsplan Sociaal Domein) komt het onderwerp privacy iets uitgebreider aan de orde. Daar is vastgelegd dat in het gesprek met inwoners wordt duidelijk gemaakt hoe er met gegevens wordt omgegaan. Zij krijgen te horen hoe de gemeente gegevens heeft beveiligd en wie er inzage heeft en waarom. Verder noemt deze subnota het inzage-

[2] Informatiebeveiligingsbeleid Gooise Meren. December 2016.

en correctierecht en de privacy op de fysieke plekken waar gesprekken tussen gemeente en inwoners plaatsvinden.

In de nota *Informatiebeveiligingsbeleid* van eind 2016 is hoofdstuk 5 gewijd aan 'Beveiliging van personeel'. Hierin wordt gewezen op het belang van menselijk gedrag bij het zorgvuldig omgaan met informatie. Enkele van de uitgangspunten die hier worden genoemd zijn:
- de verantwoordelijkheid van de lijnmanager;
- medewerkers die met vertrouwelijke of geheime informatie omgaan zijn verplicht een VOG te overleggen;
- voorlichting aan medewerkers over procedures en regels;
- het regelmatig herhalen van voorlichting om het privacybewustzijn op peil te houden;
- bij inbreuk op regels moeten gebruikelijke disciplinaire maatregelen worden genomen, zoals genoemd in het Ambtenarenreglement en gemeentelijke regels.

Het *Informatie en Automatiseringsplan 2016-2020* van de gemeente geeft de richting aan de ontwikkeling van de informatievoorziening en automatisering in de nieuwe gemeente Gooise Meren. In 2016 en 2017 gaat de aandacht uit naar 'de basis op orde'. Vanaf 2018 wordt gewerkt aan het oppakken van nieuwe ontwikkelingen. In dit verband wordt gerefereerd aan het sociaal domein, zonder hier verder op in te gaan. Daarnaast wordt informatieveiligheid als aandachtspunt genoemd en gewezen op de 'zachte factor': medewerkers moeten informatiebewust en digitaal volwassen worden gemaakt. De CISO heeft hierbij de regierol, maar het eigenaarschap ligt bij het management en de medewerkers zelf. Dit punt wordt in het Informatie en Automatiseringsplan 2016-2020 verder niet uitgewerkt.
Verder heeft de gemeente in december 2016 een *Protocol afhandeling datalekken* opgesteld. Hiermee wordt uitvoering gegeven aan nieuwe regelgeving binnen de Wet bescherming persoonsgegevens (Wbp).
De door de Vereniging van Nederlandse Gemeenten (VNG) opgestelde BIG bevat een groot aantal normen waaraan de gemeentelijke informatiebeveiliging zou moeten voldoen. Elke gemeente wordt geacht een toets uit te voeren of dat het geval is. Dit wordt een ‘GAP analyse’ genoemd. De uitgevoerde toets voor de Gooise Meren heeft geresulteerd in een actielijst van diverse maatregelen waaraan gewerkt moet worden om aan die normen te voldoen. Gesteld kan worden dat de BIG de lat voor gemeenten hoog legt, door de grote hoeveelheid normen waaraan voldaan dient te worden. Daarbij wordt bovendien geen onderscheid gemaakt tussen meer of minder urgente normen. Hoewel de gemeente Gooise Meren niet aan alle normen in de BIG voldoet, blijkt uit de GAP analyse dat er ook geen grote of urgente problemen bestaan.

Het binnen de gemeente Gooise Meren vastgelegde beleid concentreert zich op informatiebeveiliging. Privacybeleid wordt als onderwerp weinig uitgewerkt, hoewel in verschillende van deze gemeentelijke stukken het perspectief van inwoners aan de orde komt en daarnaast het belang van privacybewustzijn en gedrag van medewerkers wordt onderkend als kritische factor: 'Het gaat ook niet alleen om ICT: verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid'.[3] In de gevoerde gesprekken met diverse functionarissen binnen de gemeente is steeds benadrukt dat op verschillende wijze aandacht wordt besteed aan het (versterken van het) privacybewustzijn binnen de organisatie. Zo is herhaaldelijk genoemd dat, indien medewerkers van mening zijn dat onnodig veel informatie wordt gedeeld, hier direct aandacht voor wordt gevraagd.

[3] Informatiebeveiliging Gooise Meren. December 2016.

In de AVG, die zoals eerder opgemerkt, in de loop van 2018 toegepast moet worden, is onder meer opgenomen dat binnen elke gemeente een ‘Functionaris Gegevensbescherming’ (FG) aangewezen moet worden. In de gevoerde gesprekken is geregeld aan de orde geweest dat zodra deze FG is aangesteld, deze ook nadrukkelijk de verantwoordelijkheid zal krijgen voor het formuleren en in de praktijk brengen van het privacybeleid. De gemeente Gooise Meren onderzoekt momenteel met enkele andere gemeenten in de regio de mogelijkheden voor het gezamenlijk aanstellen van zo’n FG.

De USD werkt op basis van het informatiebeveiligingsbeleid en - plan dat voor de Wijzer is opgesteld in 2015. Recent is door de CISO een beknopt *Evaluatie en verbeterplan* opgesteld, waarin is nagegaan welke actiepunten uit 2015 zijn gerealiseerd en welke nog open staan. Ook zijn in dit document nieuwe aandachtspunten opgenomen die verband houden met nieuwe wet- en regelgeving, de nieuwe organisatie en nieuwe ontwikkelingen. Deze worden nog uitgewerkt in een nieuw Informatiebeveiligingsplan voor de USD dat dit jaar nog wordt opgesteld en dat ook past in het algemeen gemeentelijk beleid.[4] De CISO heeft aangegeven dat de fusie en de eisen van de BIG nog zoveel werk eisen om 'orde op zaken' te stellen, dat dit USD-plan wellicht in de tijd wordt doorgeschoven.

De afdeling hanteert een autorisatieprocedure waarvan de uitkomsten zijn vastgelegd in een *autorisatiematrix*. Dit betekent dat alleen geautoriseerde medewerkers toegang kunnen krijgen tot bepaalde gegevens en anderen niet.

Meer gericht op gedragsaspecten (privacy) hanteert de gemeente de *Regeling ambtelijke integriteit en gedragscode,* waarin een artikel is opgenomen over omgaan met vertrouwelijke informatie.
Voor de USD geldt bovendien het *Privacy Protocol Sociaal Domein*, waarin wordt ingegaan op principes en begrippen uit de Wet Bescherming persoonsgegevens zoals toestemming, inzage- en correctierecht, verstrekking aan derden en hoe daarmee in de concrete uitvoeringspraktijk moet worden omgegaan. De USD hanteert ook de *10 Gouden Regels*: de plichten die de medewerker moet nakomen bij het gebruik van informatie, -systemen en netwerken. Het privacyprotocol en de 10 ‘Gouden Regels’ zijn in bijlage opgenomen.
Voor de uitvoering van de Participatiewet is een *Protocol voor huisbezoeken* opgesteld. Naast diverse procedurele richtlijnen wordt in dit protocol ook ingegaan op de wettelijke kaders waarbinnen een huisbezoek plaatsvindt. In dat verband wordt aangegeven welke waarborgen voor de persoonlijke levenssfeer van belang zijn.

Vraag 1.2. Hoe wordt er geanticipeerd op de AVG?
De betrokken medewerkers binnen de gemeente zijn bekend met de AVG en oriënteren zich op de verplichtingen die daaruit zullen voortvloeien. Zo bestaat er een *Plan van Aanpak AVG*, opgesteld door de CISO. Dit plan is in juli 2016 vastgesteld. In de gesprekken is aangegeven dat dit actieplan thans in uitvoering is.

Vraag 1.3. In hoeverre voldoet het beleid aan de wettelijke grondslagen?
Het gemeentelijk beleid voldoet momenteel aan de wettelijke eisen. Tegelijkertijd is binnen de gemeente onderkend dat bepaalde onderdelen nog uitwerking behoeven. Eerder is al genoemd dat de gemeente niet aan alle normen van de BIG voldoet. De AVG, die vanaf mei 2018 zal moeten worden toegepast, zal ook nog om verschillende aanscherpingen in het beleid vragen.

[4] Verbeterplan en evaluatie. Informatiebeveiligingsplan Wijzer/USD. Maart 2017

2. Hoe is het beleid uitgewerkt en geborgd in processen?
Het vastgelegde beleid is nog weinig uitgewerkt in concrete processen en procesbeschrijvingen. Wat ontbreekt is het uitwerken van de verschillende activiteiten, het aanwijzen van functionarissen binnen de organisatie die daar uitvoering aan geven en welke gegevens concreet worden vastgelegd. Zowel de huidige Wbp als de AVG vragen hier wel om. Dit is ook binnen de gemeente zelf gesignaleerd, zoals is af te leiden uit tabel 2.2. van het *Verbeterplan en evaluatie* van maart jl.. Hier staat als nog openstaand actiepunt punt 4 aangegeven: “Per proces wordt de gegevensverwerking (doel, grondslag, welke gegevens), de risico's, de beheermaatregelen privacy en beveiliging, de instructies en de autorisaties beschreven." Wanneer de afdeling deze exercitie met de betrokken medewerkers oppakt, kan dat het privacybewustzijn en de kennis over de AVG vergroten.
In diverse gesprekken hebben medewerkers van de gemeente benadrukt dat er in de dagelijkse praktijk de nodige aandacht is voor privacy en dat medewerkers elkaar aanspreken op een juist gebruik van systemen.

3. Hoe is de toegang tot dossiers (autorisaties) geregeld?
We beantwoorden deze vraag voor de toegang tot geautomatiseerde systemen en de toegang tot dossiers en papierstroom.

Geautomatiseerde systemen
Voor de toegang tot geautomatiseerde systemen bestaat er binnen de gemeente een autorisatieprocedure. Het afdelingshoofd bepaalt volgens de zogenaamde checklistprocedure welke medewerker een autorisatie verkrijgt voor een specifiek systeem, en welke bevoegdheden deze medewerker dan heeft binnen dat systeem. De applicatiebeheerder realiseert vervolgens de toegang voor de medewerker op basis van een *autorisatiematrix* en houdt dit bij in de gebruikersadministratie. Uitdiensttreding en verandering van functie worden door het afdelingshoofd doorgegeven aan de applicatiebeheerder die vervolgens de noodzakelijke aanpassingen doet. Deze werkwijze was al van kracht in de oude situatie, de nieuwe gemeente gaat hem nu gemeentebreed implementeren. Het voornemen bestaat om aan de afdeling P&O (HRM) de verantwoordelijkheid te geven voor het doorgeven van personele wijzigingen. Daarnaast is het zo dat het afdelingshoofd als houder van de administratie en proceseigenaar bepaalt welke type functionarissen en soms specifieke personen in verband met hun taak toegang moeten hebben.

Over de toegang tot de specifieke systemen is het volgende op te merken. De vraagverkenner en vraagverhelderaar die aan het begin van het proces een rol hebben, werken met het regiesysteem Topicus. De vraagverhelderaar legt daarin verslagen van gesprekken vast en het Plan van Aanpak. De specialisten hebben eveneens toegang tot dit systeem, maar dan alleen ter inzage. Zij kunnen daarin alle cliënten sociaal domein raadplegen waarover de vraagverkenner of de vraagverhelderaar gegevens heeft ingevoerd. De bedoeling is dat zij dit systeem alleen raadplegen voor hun eigen cliënt. Om ongeoorloofde raadpleging te voorkomen, zijn er twee controlemechanismen ingebouwd. Zodra Topicus is geraadpleegd, wordt dit gelogd en gemeld op het scherm van de vraagverhelderaar. Zo ziet deze wie welke cliënt in Topicus heeft geraadpleegd. Dergelijke logging maakt het ook mogelijk om achteraf te checken of de raadpleging rechtmatig was, maar dit wordt niet (structureel) gedaan, omdat de vraagverhelderaar als eerste kan signaleren wie er wellicht onrechtmatig een cliëntdossier raadpleegt. Dit wordt beschouwd als een voldoende rem op ongeoorloofde raadpleging.

De vraagverhelderaar schuldhulpverlening heeft ook het systeem Mesis ter beschikking. Dat wordt gebruikt om bij mensen met financiële problemen te bepalen of zij kansrijk zijn om een schuldhulpverleningstraject te doorlopen. De uitkomsten van deze test worden in Topicus gezet, zodat de specialist schuldhulpverlening ermee aan de slag kan.

Daarnaast heeft de vraagverhelderaar Participatie het systeem Competensys, een diagnose instrument voor re-integratie. Dit wordt toegepast bij cliënten van de Participatiewet. De uitkomsten van deze test worden ook in topics opgeslagen, zodat de re-integratie specialist daarmee verder kan.

De specialisten Jeugdwet, Wmo, Participatiewet en Schuldhulpverlening en de administratieve krachten werken met GWS-Suite, een cliëntvolgsysteem waarin de elektronische cliëntdossiers worden opgebouwd. De administratieve krachten 'maken een cliënt aan' in het systeem en voegen informatie toe uit toegestuurde documenten. Het dossier wordt doorgezet naar het betreffende specialistenteam, waar het in de algemene werkvoorraad komt. De specialist kan een zaak op zijn eigen naam zetten en vervolgens in GWS verder aan het dossier werken. Iedereen binnen een team heeft inzagerechten voor de totale werkvoorraad. Dat is zo geregeld om het overnemen van elkaars cliënten te vergemakkelijken. Binnen de 'regeling' is het afhankelijk van je functie tot welke schermen je toegang hebt. Ook hier zou achteraf aan de hand van de loggegevens gecheckt kunnen worden in hoeverre consulenten zich houden aan raadpleging van de gegevens van de eigen cliënten. Dit wordt voor zover gebleken is in het onderzoek niet (structureel) gedaan. Vanwege de strenge toegangsbepalingen tot de digitale systemen (geregeld in de autorisatiematrix) wordt door de medewerkers aangenomen dat er niet tot nauwelijks sprake is van ongeoorloofde raadpleging.

De medewerkers die de Participatiewet uitvoeren hebben nog de beschikking over Suwinet. Suwinet is een infrastructuur waarmee de uitvoerders van de socialezekerheidswetten gegevens van hun cliënten kunnen inzien die bij andere instanties zijn opgeslagen. Zo kunnen de uitvoerders van de Participatiewet de gegevens raadplegen die over hun cliënt al bij andere overheidsbronnen zijn vastgelegd en die nodig zijn voor de uitvoering van de wet. Het gaat om bijvoorbeeld over gegevens over inkomen en uitkering, arbeidsverleden, autobezit, bezit onroerend goed, studiefinanciering, diploma's etc. Het gebruik van Suwinet is geregeld in de wet Suwi en onderliggende regelgeving en moet voldoen aan normen die door de Suwipartijen (SVB, UWV, gemeenten) zijn opgesteld.
In Gooise Meren is het gebruik van Suwinet uitgewerkt in procedures voor autorisaties en controles op naleving. Het afdelingshoofd autoriseert en de applicatiebeheerder voert uit en houdt de gebruikersadministratie bij. De lograpportages worden achteraf strikt gecontroleerd op afwijkende zoekpatronen, eerst door de applicatiebeheerder en vervolgens door de CISO. Zo nodig worden medewerkers bevraagd op hun zoekgedrag. Uit onderzoek van de Inspectie SZW over 2015 bleek dat in de gemeente aan alle onderzochte Suwinet-normen werd voldaan, alleen moest de toegang voor schuldhulpverlening worden afgesloten. Dat is meteen gebeurd.

Ten slotte kan hier nog worden opgemerkt dat de afdeling zelf het werken met beveiligde email (Zivver) heeft geïnitieerd. In essentie behelst deze applicatie dat het systeem automatisch controleert of er mogelijk vertrouwelijke gegevens in een e-mail worden opgenomen. In dat geval wordt de steller automatisch gevraagd of de e-mail via Zivver moet worden opgesteld en verzonden. Als dat het geval is heeft de ontvanger een extra autorisatiecode nodig om de mail te kunnen openen. Deze werkwijze voorkomt dat eventueel verkeerd geadresseerde e-mails door derden kunnen worden gelezen

Papierstroom
Naast de digitale dossiers en gegevensstroom vindt er veel informatieuitwisseling ‘op papier’ plaats. De gemeente wil op termijn starten met het digitaliseren van de informatiestromen, op het moment van onderzoek was dat nog niet zo ver.[5]

[5] De start heeft op 4 september jl. plaatsgevonden met het vaststellen van een plan van aanpak.

De post komt binnen bij de postkamer. Post geadresseerd aan de USD wordt niet door de postkamer opengemaakt. De post voor de USD (aanvraagformulieren, kopieën van bewijsstukken en ID-bewijzen etc.) komt terecht bij de administratieve krachten (AK) van de USD. Zij checken de documenten op volledigheid (bv. een aanvraag op ondertekening en verplichte bijlagen), en sturen het door naar de betreffende specialist of team. De AK heeft ook toegang tot Suwinet; zij maken namelijk een uitdraai voor de handhavers Participatiewet die op grond daarvan onderzoek doen voordat het dossier naar de inkomensspecialist gaat. De specialisten maken de beschikking; daarna komt het dossier terug bij de AK die het archiveert.

De re-integratiespecialisten zijn gehuisvest in een apart kantoor. Zij ontvangen op papier van het UWV uitkomsten van uitgevoerde loonwaardebepalingen en brieven over opname van een cliënt in het doelgroepenregister. Deze berichten worden in ordners opgeborgen. Hoewel het gaat over gegevens over de gezondheidssituatie van burgers (belastbaarheid en arbeidsmogelijkheden), dus bijzondere gegevens in de zin van de Wbp, zijn er geen specifieke afspraken over hoe je moet omgaan met deze gegevens. Dat geldt ook voor gegevens over de gezondheid van de cliënten Participatiewet die in GWS of een papieren dossier worden opgeslagen.

4. Hoe ziet het toezicht op de omgang met de persoonsgegevens er uit?
De verantwoordelijkheden, rollen en taken met betrekking tot de omgang met persoonsgegevens zijn in het *Informatiebeveiligingsplan* van de gemeente vastgelegd.

Het afdelingshoofd is er verantwoordelijk voor dat er met persoonsgegevens zorgvuldig wordt omgegaan. Het toezicht daarop wordt allereerst uitgevoerd de kwaliteitsmedewerker (dossiers) en de interne controller (procesniveau, bestandscontroles). Dit gebeurt op basis van het *Interne controleplan.*[6] Hierin is onder meer aangegeven welke controles plaatsvinden en op welke onderwerpen wordt gecontroleerd. Privacy is niet een apart aandachtspunt in het Controleplan. Bij aanvang van de decentralisaties hebben de kwaliteitsmedewerkers bij de toetsing extra veel aandacht besteed aan de gegevensverwerking, met name in verband met de implementatie van de jeugdwet. Onder meer heeft de kwaliteitsmedewerker Jeugd hiertoe een speciale kenniswebsite ingericht die veel informatie over privacy bevat.
Door de kwaliteitsmedewerker wordt bij het controleren van dossiers nog steeds gelet op mogelijk overbodige informatie.
Los hiervan vindt controle plaats op Suwi-raadplegingen. Hiervoor dienen de lograpportages, die in eerste instantie worden bekeken door de applicatiebeheerder en vervolgens door de CISO. De lograpportages van de twee klantvolgsystemen Topicus en GWS worden niet (structureel) gecontroleerd. Wel ziet de vraagverhelderaar wie welke cliënt in Topicus heeft geraadpleegd wat voor dit systeem een rem zet op ongeoorloofde raadpleging.

Controle op het gebruik van het Digitaal Leefplein wordt uitgevoerd door de beheerder van RGV.
De tweedelijns controle wordt uitgevoerd door de CISO's. Zoals eerder aangegeven moeten de CISO's eerst nog de basis op orde zien te krijgen, voordat zij zich met specifieke controles binnen de afdelingen bezig kunnen houden. Voor de USD zijn zij voorlopig alleen bij controle van de Suwinet-loggings betrokken.

De verbijzonderde interne controle valt onder de concern controller. Hoewel deze controle nog vooral op financiële risico's is gericht, is het plan om te zijner tijd ook aan privacyrisico's aandacht te gaan besteden.

[6] Intern Controleplan, september 2016.

5. Hoe gaat het in de praktijk, op de werkvloer?
Uit de beschrijvingen in deze rapportage wordt tot dusverre duidelijk dat er sterke verwevenheid is tussen het beleid van de Gooise Meren inzake informatiebeveiliging en privacy. Door veel procedures vast te leggen in systemen en applicaties, geeft dit ook richting aan de omgang met vertrouwelijke gegevens in de praktijk. In dit kader kan bijvoorbeeld worden gewezen op het goede en intensieve gebruik van de autorisatiematrix en de toepassing van extra beveiligde mail (Zivver). Uit het onderzoek is naar voren gekomen dat dat er in de praktijk geen vaste afspraken zijn over de manier waarop op de werkvloer consequent invulling en gevolg wordt gegeven aan het vastgelegde beleid. In verschillende gesprekken is door medewerkers benadrukt dat zij zich zeer bewust zijn van het belang om hier goede aandacht aan te besteden. De medewerkers van Gooise Meren zijn er zich van bewust dat zij te maken hebben met informatie die deel uitmaakt van de persoonlijke levenssfeer van de cliënten. Daarmee ervaren zij de verantwoordelijkheid om hier vertrouwelijk mee om te gaan. Binnen de organisatie is er aandacht dat louter informatie wordt verzameld die van belang is voor het tegemoet komen aan de ondersteuningsbehoefte van de cliënt ('need to know'). Als extra informatie ('nice to know') wordt vastgelegd, spreken medewerkers hier elkaar op aan. Indien medewerkers de indruk hebben dat collega's te weinig privacybewust zijn, is de praktijk dat zij er elkaar op aanspreken. Dit geldt met nadruk ook voor de informatie die via het Digitaal Leefplein wordt uitgewisseld. In die zin is er aandacht voor dat niet louter volstaan kan worden met het reguleren van het gewenste gedrag door middel van procedures en applicaties.

6. In hoeverre voldoet de uitvoering aan de wettelijke normen en de onder 1 genoemde wettelijke kaders?
De uitvoering voldoet momenteel aan de wettelijke normen en kaders. Wel kan de uitvoering op verschillende onderdelen worden aangescherpt. Dit is voorzien in het Verbeterplan en in de voorbereiding op de AVG. Het scherper inregelen van de toegang tot systemen, zodat medewerkers alleen toegang hebben tot hun eigen cliëntenbestand, dient nog uitgewerkt te worden. Verder zou er, als de AVG toegepast moet worden, door middel van loggings structureel moeten worden nagegaan of medewerkers alleen gegevens inzien die voor hun werk relevant zijn. Ook dient de informatieverstrekking met betrekking tot hun (inzage- en correctie-)rechten en plichten aan de burgers verbeterd te worden.

7. In hoeverre heeft de gemeente een balans gevonden tussen regels en procedures rondom de bescherming van privacy enerzijds en een goede dienstverlening aan de burger anderzijds waarbij zij de hulp krijgen die nodig is?
Geregeld moeten medewerkers informatie overdragen aan anderen binnen de organisatie of aan instanties die invulling gaan geven aan de ondersteuningsbehoefte van cliënten. Zij moeten daarbij voldoen aan de wettelijke vereisten rondom privacy en steeds opnieuw vaststellen dat zij privacygevoelige informatie mogen overdragen. Ook mogen zij louter informatie verzamelen die relevant is voor de ondersteuningsbehoefte van de cliënt. Tegelijkertijd hebben cliëntondersteuners en zorgaanbieders voldoende informatie nodig voor een goede invulling van hun verantwoordelijkheid. En willen cliënten niet steeds opnieuw hun verhaal doen.
Medewerkers zijn zich naar eigen zeggen bewust van deze tweestrijdigheid en stellen daarin de juiste balans te hebben gevonden. Zij gaan vertrouwelijk om met persoonlijke informatie en wegen af welke informatie noodzakelijk is om over te dragen. Ook wordt er naar gestreefd dat cliënten niet keer op keer dezelfde informatie hoeven te verstrekken.
Met iedere nieuwe cliënt wordt een gesprek gevoerd aan de hand van de zelfredzaamheidsmatrix. Deze is bedoeld voor mensen met multi-problemen. De afdeling heeft nu onderkend dat de meeste burgers een enkelvoudige vraag hebben en dat met (veel) minder gegevens de aanvraag kan worden

afgehandeld. De afdeling gaat daarom zijn processen herinrichten, waarmee de gegevensverwerking meer in verhouding is met de situatie waarin cliënten verkeren.[7]

Vertegenwoordigers van cliëntenorganisaties beantwoorden de vraag of er sprake is van een goede balans in de hoeveelheid te verstrekken informatie kritischer. Enerzijds ervaren zij dat zij veel informatie moeten verstrekken, waarvan zij soms het idee hebben dat onderdelen van die informatie niet relevant zijn voor hun vraag. Ook ervaren zij dat zij geregeld dezelfde informatie opnieuw moeten verstrekken.

2.3 Leren en verbeteren

Context en bevindingen
Privacy als onderwerp is bij de USD aan de orde als er een aanleiding voor is, zoals in de aanloop naar de decentralisaties en bij de introductie van Zivver, het beveiligde e-mailprogramma.
Betrokkenen stellen dat de basis voldoende geborgd is en het daarom alleen nodig is om privacy op de agenda te zetten als er een concrete aanleiding voor is. Zij vinden het niet nodig om privacy periodiek op de agenda te zetten. In enkele gesprekken werd gesteld: 'Je weet dit soort dingen gewoon', 'Het is er in gehamerd'.
Eerste vraagbaak voor vragen over privacy is de kwaliteitsmedeweker. Het komt soms voor dat de kwaliteitsmedewerker de jurist van de Regio GV raadpleegt. Dit gebeurt op informele basis, aangezien deze jurist geen officiële rol meer heeft voor de afzonderlijke gemeenten. Sommige medewerkers menen echter dat zij nog steeds benaderd kan worden voor advies.

Medewerkers voelen zich voldoende geëquipeerd om in de uitvoering zorgvuldig met privacy om te gaan. Door velen is er op gewezen dat de systemen door middel van autorisaties en vastgelegde procedures de zorgvuldige omgang met privacy min of meer ‘afdwingen’.
Hierdoor is het gevoel ontstaan dat privacy al goed belegd is in de organisatie. Bovendien wordt genoemd dat bij de voorbereiding op de decentralisaties veel aandacht is besteed aan het borgen van de privacy. Geregeld is daar in de gesprekken aan toegevoegd dat daardoor de noodzaak ontbreekt om vandaag de dag het onderwerp structureel binnen de organisatie te agenderen. Dat zou bijvoorbeeld kunnen door vaste agendering van het onderwerp in het werkoverleg of het aanbieden (en min of meer verplicht stellen) van ‘opfriscursussen’. Door medewerkers van de gemeente is gesteld dat dergelijke acties vooralsnog niet nodig zijn, aangezien het beleid pas enkele jaren in werking is.
Vanuit cliëntenorganisaties is aangegeven dat de gemeente cliënten beter moet informeren over het waarom van de gegevensopvraag en wat er met de gegevens gebeurt. Ook is dat eerder zowel in het verband van de Adviesraden aan de gemeente gemeld, als in het programma Samenkracht! In het onderzoek is niet gebleken dat dergelijke signalen binnen de organisatie structureel worden opgepakt.

Deze signalen en de aanscherping van de regelgeving door de AVG kan voor de afdeling aanleiding zijn om hernieuwde aandacht te besteden aan het onderwerp privacy. Ook kan het relevant zijn voor medewerkers die recent in dienst zijn gekomen en die daarom de aandacht voor privacy die er rondom de decentralisaties is geweest niet hebben meegekregen.

7 De zelfredzaamheidsmatrix beoordeelt aan de hand van 11 domeinen van het dagelijks leven de mate van zelfredzaamheid. In een gesprek met de cliënt vraagt de hulpverlener of beoordelaar naar de huidige situatie op 11 levensdomeinen, naar eventuele problemen en wat de persoon doet om die problemen op te lossen. De 11 domeinen zijn: Financiën, Dagbesteding, Huisvesting, Huiselijke relaties, Geestelijke gezondheid, Lichamelijke gezondheid, Verslaving, Activiteiten Dagelijks Leven, Sociaal netwerk, Maatschappelijke participatie en Justitie

Een andere aanleiding is het in gebruik nemen van het nieuwe gebouw van de gemeente. In de grotere flexruimten zal er nog meer aandacht moeten zijn voor het beschermen van vertrouwelijke gegevens die op een bureau kunnen liggen, die op schermen zichtbaar kunnen zijn of die gedurende telefoongesprekken, waar collega's bij zijn, genoemd kunnen worden.
In de gesprekken is niet gebleken dat het anticiperen op dergelijke veranderingen binnen de organisatie proactief wordt opgepakt. Eerder is er sprake van een afwachtende houding, waarbij gewezen wordt op de uitvoering van actieplannen van de CISO (die aangegeven hebben weinig capaciteit te hebben) en de komst van de mogelijk in regionaal verband aan te stellen FG. Ook wordt er gewezen op het feit dat de verbouwing nog niet klaar is. Er zijn een aantal zaken geregeld (zoals een clean desk policy), maar het concept van flexwerken en wat dat betekent voor privacy moet zich nog uitkristalliseren.

8. Op welke manier worden medewerkers betrokken bij, en getraind in het borgen van de privacy en het versterken van de informatieveiligheid?
Privacy wordt binnen de teams aan de orde gesteld als er een concrete aanleiding voor is. Het is geen regulier terugkerend onderwerp van bespreking.

De decentralisaties en de daarbij behorende nieuwe werkwijze en systemen waren een aanleiding om in het recente verleden privacy op de agenda te zetten. Recent is privacy aan de orde gekomen toen Zivver werd geïntroduceerd, de veilige manier van mailen. Ook bij het inwerken van nieuwe medewerkers is zorgvuldig omgaan met persoonsgegevens een onderwerp. Zo is iedereen geïnformeerd over clean desk policy, het afsluiten van je pc als je je werkplek verlaat, bij de printer blijven als je print, vernietigen van papier, geen informatie geven aan niet-cliënten.

De specialisten Jeugdwet en Wmo geven aan bij vragen en onduidelijkheden over privacy navraag te doen bij de kwaliteitsmedewerker. En als die het niet weet, kan volgens hen de jurist van de Regio GV geraadpleegd worden. Tevens staan de betrokken medewerkers landelijke kennisbanken ter beschikking waar de gemeente op is geabonneerd.

Medewerkers Participatiewet kunnen worden aangesproken door de applicatiebeheerder/CISO wanneer de lograpportages Suwinet een afwijkend patroon laten zien. Bij het volgsysteem Topicus kan de vraagverhelderaar zien welke collega's welke dossiers hebben geraadpleegd. Zowel bij Topicus als bij GWS worden raadplegingen wel gelogd, maar daar wordt niet structureel op gecontroleerd.
Medewerkers kunnen ook aangesproken worden door de kwaliteitsmedewerker als er uit de dossiers blijkt dat er teveel informatie is opgenomen.

De CISO's hebben opgemerkt dat zij privacy als onderwerp binnen de afdelingen aan de orde willen stellen. Vooralsnog is daar geen tijd voor geweest, maar het staat wel op de actiepuntenlijst.
Daarnaast heeft de jurist van de RGV het plan om in het verlengde van het zojuist verschenen rapport over grondslagen en toestemming[8], een juridische toolkit te ontwikkelen waarvan de gemeente indien gewenst gebruik kan maken. Naar haar mening blijkt uit dit onderzoek dat de aandacht voor privacy nog extra bevorderd moet worden.
Ook vanuit het team Bedrijfsvoering van de USD is aangegeven dat het rapport over grondslagen aanleiding is om het onderwerp te agenderen, evenals het nieuwe en aangescherpte controleplan.

[8] Grondslagenonderzoek verwerking persoonsgegevens in het sociaal domein. Regio Gooi en Vechtstreek. Maart 2017

9. Op welke manier heeft de gemeente het proces van evalueren en verbeteren ingericht?
Voor elk beleid geldt dat het nuttig is om goede aandacht te hebben voor evaluatie en ‘leren en verbeteren’. In de context van de AVG wordt ook nadrukkelijk gesteld dat gemeenten een ‘Plan-Do-Check-Act’-cyclus dienen in te richten, waarin structureel aandacht is voor ‘leren en verbeteren’. Met het inrichten van deze cyclus heeft de gemeente onlangs een eerste begin gemaakt in de vorm van de GAP-analyse op de normen die in de BIG zijn gesteld. Dat heeft geleid tot een planning met prioriteiten. Na deze 'plan'-fase gaan de CISO's nu starten met de implementatie (de 'act'-fase). Het is de bedoeling om in de toekomst deze aanpak te verbreden naar ook andere normstellingen dan de BIG, en op deze manier structurele aandacht te hebben voor verbeteracties.

10. Is er al een evaluatie geweest en hoeverre heeft dat tot verbeteringen geleid?
Binnen de gemeente is het privacybeleid niet structureel geëvalueerd. In dat verband kan worden opgemerkt dat de gemeente zelf nog relatief kort bestaat. Bovendien hebben de decentralisaties in het sociaal domein ook pas korte tijd terug hun beslag gekregen. In dat licht, zo stellen medewerkers van de gemeente, zou het ook wat kort dag zijn om evaluaties in te richten en uit te voeren.

2.4 Positie burger

Context en bevindingen
Met de komst van de AVG worden de rechten van burgers aangescherpt. Maar ook de huidige Wbp geeft expliciete rechten aan burgers ten aanzien van hun eigen persoonsgegevens. Onder andere gaat het om het recht op informatie: welke gegevens worden opgevraagd, met welke doel en aan wie worden ze verder verstrekt en met welke reden. Daarnaast hebben burgers recht op inzage, correctie en verwijdering van gegevens.
Deze rechten moeten ook daadwerkelijk kunnen worden gerealiseerd. Dat wil zeggen dat de informatie daarover vindbaar en begrijpelijk moet zijn, en dat er wordt aangewezen hoe de toegang tot de rechten mogelijk is (waar kan ik mijn gegevens corrigeren, wat moet ik daarvoor doen).

Het omgekeerde hiervan is dat de betrokken organisatie, in dit geval de gemeente in het bijzonder de USD, (actieve) informatieplicht heeft jegens de burger (art. 33 en 34 Wbp). Hoe gevoeliger de gegevens des te meer de gemeente in detail moet informeren over het hoe en waarom van de gegevensverwerking.

Over de positie van de burger is informatie terug te vinden in het Privacyprotocol, die onder meer op de website van de gemeente aangetroffen kan worden. Maar er wordt zowel op de website, als in gesprekken en folders te weinig in begrijpelijke taal uitgelegd wat dat betekent in hun concrete situatie. Dat komt wellicht omdat binnen de organisatie de ervaring is dat cliënten zelden om een toelichting vragen op hun rechten of om inzage in de door de gemeente over hun vastgelegde gegevens. Als eerder opgemerkt is er binnen de organisatie geen functionaris aan te wijzen die het initiatief zou kunnen nemen om de processen vanuit de positie van de burger kritisch te beschouwen en deze waar nodig geacht op dat punt te versterken. De CISO’s hebben weliswaar informatiebeveiliging in hun portefeuille, maar geen expliciete taak aangaande privacy, en nog minder als het gaat om actieve voorlichting aan cliënten. Dat zou in de portefeuille van een Functionaris Gegevensbescherming (verplicht onder de AVG) horen; over een aanstelling van een dergelijke functionaris bestaat, zoals eerder al opgemerkt, nog geen zekerheid.
In het *Privacyprotocol* dat op de website van de gemeente is te vinden (en in de bijlage is opgenomen) komen de rechten van de burger wel aan de orde, maar dan ook weer vanuit de invalshoek van de organisatie. Er staat in het protocol onder andere dat inzage en correctierecht schriftelijk moeten

worden aangevraagd bij de behandelend ambtenaar. In de *Wijzer-folders* staan algemene zinnen over het navolgen van de privacywetgeving door de gemeente.

Op de *website* wordt verder verwezen naar beleidsstukken. Dergelijke beleidsstukken richten zich vooral op de organisatie en zijn op zichzelf weinig toegankelijk en begrijpelijk voor cliënten. Deze informatie verschaft hen geen korte en krachtige informatie over wat er met de eigen persoonsgegevens gebeurt en wat hun rechten zijn.
Overigens heeft de afdeling zelf bij de gemeente aangekaart om informatie over het onderwerp 'privacy sociaal domein' op de site te zetten. In de huidige systematiek van de website, wordt vooral informatie aangeboden waar veel mensen naar zoeken. Zolang privacy nauwelijks zoekacties van burgers oproept, blijft de informatie moeilijk vindbaar.

Naar mening van vertegenwoordigers van cliëntenorganisaties is de positie van de burger onderbelicht, zowel in beleid, in de uitvoering als in informatie voor de burger. Daarmee blijft ook het belang van de rechten van de burger onderbelicht.

11. Wanneer en op welke manier geven burgers toestemming voor het gebruik en verwerken van gegevens?
Er wordt aan burgers bij een aanvraag voor een voorziening schriftelijk toestemming gevraagd voor het uitwisselen van gegevens met derden.

De toestemming komt aan de orde bij het gesprek met de cliënt, doorgaans als het tot een aanvraag komt waarbij nadere informatie moet worden opgevraagd of doorgegeven. De toestemmingsverklaring wordt uitgereikt aan de cliënt waarna wordt toegelicht waarom gegevens moeten worden uitgewisseld met derden. De toestemmingsverklaring moet worden ondertekend door de cliënt.
Er zijn drie formulieren voor het geven van toestemming door middel van ondertekening door de cliënt: een formulier voor Wmo-voorzieningen, een voor de Jeugdwet en een voor schuldhulpverlening.

De *Toestemmingsverklaring voor het uitwisselen van gegevens* voor een aanvraag Wmo bevat een korte toelichting, dat, om het onderzoek naar de ondersteuningsvraag goed te kunnen uitvoeren, het nodig is om gegevens uit te wisselen. Vervolgens staan er een aantal instanties genoemd; de specialist of vraagverhelderaar kruist aan met welke instantie gegevens worden uitgewisseld (opgevraagd en ontvangen). Ook wordt aangegeven, dat indien zorg wordt ingezet, gegevens worden doorgegeven aan zorgaanbieders.
De *Toestemmingsverklaring Jeugdhulp* behorend bij de aanvraag of melding van een voorziening Jeugdwet is uitvoeriger en bevat ook de precieze namen van personen waaraan informatie wordt gevraagd/verstuurd, een lijst met documenten die de cliënt overhandigt en waarvoor hij al of niet toestemming geeft voor inzage, gebruik voor relevante informatie, opname in het dossier, deling met derden. Ook wordt apart toestemming gevraagd het Plan van Aanpak te delen met een zorgaanbieder. Bij dit formulier zit een uitvoerige toelichting met juridische achtergronden. Vanwege deze juridische invalshoek zal het niet voor elke cliënt eenvoudig zijn om dit te begrijpen.
De toestemmingsverklaring schuldhulpverlening is opgenomen in de *Overeenkomst schuldhulpverlening* die de cliënt met de schuldhulpverlener aangaat. Hij geeft bij het tekenen van de Overeenkomst daarbij automatisch toestemming om overleg te voeren met en informatie op te vragen bij derden.

Bij het verwerken van een aanvraag heeft het college van B&W allerlei mogelijkheden en bevoegdheden om informatie en nadere inlichtingen in te winnen die noodzakelijk zijn bij de

beoordeling. De gemeente informeert de aanvragers niet actief over deze bevoegdheid en verstrekt hun daarmee geen overzicht van de aanvullende gegevens die worden verzameld. We nemen aan dat informatie hierover standaard is opgenomen in het (landelijk standaard) Aanvraagformulier.

Het is de ervaring van de medewerkers dat Wmo-cliënten graag de benodigde informatie verstrekken. Vaak geven ze meer dan nodig is. Stukken die niet nodig zijn of niet in het dossier hoeven te worden opgenomen, worden vernietigd. Zoals eerder is opgemerkt geven medewerkers aan dat er vanuit burgers bijna nooit vragen komen over privacykwesties.

Op dit moment wordt met nagenoeg iedere nieuwe cliënt een gesprek gevoerd aan de hand van de zelfredzaamheidsmatrix. Deze is bedoeld voor mensen met multi-problemen. De afdeling heeft onderkend dat de meeste burgers een enkelvoudige vraag hebben en dat met (veel) minder gegevens de aanvraag kan worden afgehandeld. De afdeling gaat daarom zijn processen herinrichten, hetgeen de mogelijkheid biedt om de gegevensverwerking proportioneler in te richten.

Cliëntperspectief
Door cliënten, met name bij werk & inkomen, wordt opgemerkt dat de gemeente wel heel veel gegevens vraagt, zonder dat altijd duidelijk wordt gemaakt waarom dat nodig is. De mate waarin zij daarover worden geïnformeerd hangt af van de individuele medewerker. Volgens de cliënten wordt toestemming snel gegeven, omdat je in een afhankelijke positie zit. De gemeente komt op deze manier wel heel veel van je te weten, over alle levensterreinen. Ook leden van de Wmo-adviesraad wijzen op de afhankelijke positie van cliënten, waardoor cliënten geneigd zijn veel informatie met de gemeente te delen. Dat versterkt volgens cliënten het belang dat de gemeente heeft om zich terughoudend op te stellen bij het uitvragen van gegevens. Ook omdat de gemeente geen organisatie op afstand is. Medewerkers van de gemeente kunnen cliënten in de winkel of op straat tegenkomen.

12. Op welke manier worden burgers geïnformeerd over het gebruik en de verwerking van hun persoonsgegevens?
De burgers worden geïnformeerd over de gegevensverwerking in het gesprek met de vraagverhelderaar. Daarnaast kunnen zij (vak-)informatie vinden op de website en zijn er folders met een zinsnede over het naleven van privacyregels door de gemeente.

De vraag van de burger om ondersteuning komt na de vraagverkenner terecht bij de vraagverhelderaar. Deze gaat in gesprek met de burger. De vraagverhelderaar hoort volgens de eigen werkwijze van de gemeente in dat gesprek aan de orde te stellen waarom er vragen naar de persoonlijke situatie worden gesteld en waarom deze gegevens worden vastgelegd in een verslag. Ook hoort in dat gesprek te worden aangegeven dat de betrokkene zijn eigen gegevens in zijn (digitaal en papieren) persoonsdossier kan inzien en kan (laten) corrigeren. De betrokkene krijgt een verslag van het gesprek met de vraagverhelderaar en kan volgens de medewerkers, op deze manier zien welke gegevens tijdens dit gesprek zijn vastgelegd.
In de checklist voor de Wmo-gesprekken is het verstrekken van informatie aan de cliënt over de gegevensverwerking recent als apart aandachtspunt opgenomen.

Naast de gesprekken is zijn er zogenaamde Wijzer-folders. In de *folder Algemene Informatiewijzer* en in de *folder Het Gesprek* wordt aangegeven dat de gemeente zich aan de privacywetgeving houdt en alleen informatie overdraagt aan instanties als dat nodig is voor levering van zorg, als de betrokkene toestemming geeft of als er een wettelijke basis is.

In de *Nieuwsbrief Wijzer* van september 2015 is een alinea opgenomen over 'veiligheid persoonsgebonden informatie'. Hierin wordt verwezen naar het Privacyprotocol sociaal domein dat de basis vormt voor de omgang met persoonsgegevens en het beveiligingsplan van de gemeente.
De Nieuwsbrief Wijzer van maart jl. heeft een alinea gewijd aan Zivver, de veilige e-mailverbinding om berichten te sturen naar en te ontvangen van de gemeente.

Op de *gemeentelijke website* is een pagina gewijd aan 'wat de gemeente doet om bij het gebruik van deze website uw privacy zoveel mogelijk te beschermen'. Daarbij wordt met een link verwezen naar de Wbp, naar beleidsstukken: het Informatiebeveiligingsbeleid, het Informatiebeveiligingsplan en het Privacyprotocol, en naar Zivver.

Als nieuwe voorziening voor het informeren van de burger komt er in het Digitaal Leefplein een mogelijkheid voor een eigen portal, waarmee de burger in zijn eigen dossier kan zien welke maatwerkvoorzieningen hij heeft. Bij de toekomstige digitalisering van de gemeentelijke processen krijgt de burger inzage in zijn dossier en de voortgang van een zaak die bij de gemeente loopt.

Cliëntperspectief
Volgens vertegenwoordigers van de cliënten is het afhankelijk van de individuele medewerker of en in hoeverre je wordt geïnformeerd over de gegevensverwerking. Over het inzage- en correctierecht wordt naar hun ervaring geen informatie gegeven. Er is de nodige zorg en wantrouwen over wat de gemeente doet met de gegevens, hoe lang ze die bewaart en met wie de gegevens worden gedeeld. Bij chronisch zieken speelt dit minder omdat zij niet steeds weer willen hoeven uitleggen en aantonen wat er met hen aan de hand is, maar het is vooral een zwaarwegend punt bij de (jeugd-) GGZ en Participatiewet.

In Samenkracht! is privacy een belangrijk thema dat vaker aan de orde is gekomen. Steeds is benadrukt dat gemeenten bij iedere cliënt goed moeten uitleggen hoe er met privacy wordt omgegaan en dat er ruimte is voor individuele afspraken, bijvoorbeeld over wat er wel in niet in het dossier moet komen. Samenkracht! heeft bij de USD hier aandacht voor gevraagd, onder andere naar aanleiding van de *themabijeenkomst over Privacy* en de *nota Samenkracht!.* Verder wordt nog aandacht gevraagd voor de medische gegevens die de gemeente opvraagt: het is bij cliënten onbekend hoe daarmee om wordt gegaan. Dan gaat het ook over gegevens die bij de re-integratie worden gebruikt, bijvoorbeeld uit Competentsys.

2.5 Kaderstellende en controlerende taak gemeenteraad

Context en bevindingen
Allereerst moet opgemerkt worden dat de gemeente en daarmee de raad van deze gemeente pas 1,5 jaar bestaan. Het onderwerp privacy is in de raad nog nauwelijks onderwerp van gesprek geweest. In ieder geval staat het niet regulier op de agenda en is het ook geen onderwerp bij de bestuursrapportages.
Er is vorig jaar eenmalig een gesprek geweest over de AVG. De wethouder heeft aangekondigd om met het oog op de AVG in gesprek te gaan met de auditcommissie. Wellicht kan dan besloten worden om de accountant aanvullend onderzoek te laten doen. In het recente *accountantsrapport* voor de raad over 2016 wordt informatiebeveiliging als aandachtpunt genoemd, evenals de verbijzonderde interne controle, houding en gedrag.

13. Op welke manier kan de gemeenteraad het beleid rondom privacy en informatieveiligheid in het sociaal domein controleren en sturen?
Privacy is een grondrecht van de inwoners van Gooise Meren. In de inleiding van dit rapport is dit onderbouwd en zijn ook enkele beleidsmatige risico's (zoals het opgelegd krijgen van boetes) genoemd. Vanuit die optiek ligt er een belangrijke verantwoordelijkheid van de raad. De raad dient aandacht te hebben voor de kaders van het beleid, waarmee aan huidige en toekomstige eisen wordt voldaan. Verder zou de raad kunnen stellen geregeld geïnformeerd te willen worden over risicoanalyses, normen, het bestaan van plannen van aanpak, de uitvoering daarvan, mogelijke incidenten en de wijze waarop de gemeentelijke organisatie pogingen in het werk stelt om incidenten structureel te voorkomen.[9]

14. Op welke wijze is de raad tot nu toe betrokken geweest?
De Raad is nauwelijks betrokken bij het onderwerp privacy. In de door ons gevoerde gesprekken is gesteld dat dit onderwerp meer een zaak is van bedrijfsvoering, dus van het college. Vorig jaar juni is er een bijeenkomst met de Raad geweest over privacy en het jeugdbeleid. Daarin is toen voornamelijk gesproken over de AVG. Ook is het beleidsplan sociaal domein in de raad geagendeerd geweest en is er tijdens de behandeling gesproken over privacy. De raad heeft van de Inspectie SZW het controleverslag Suwi ontvangen, maar heeft dat niet geagendeerd. Het beveiligingsbeleid is zijdelings aan de orde geweest: er is in de Perspectiefnota extra geld gevraagd voor beveiligingssoftware en er is besloten om voor de uitwijkvoorziening ICT samen te werken met Hilversum.

15. Is er in het privacybeleid van de gemeente aandacht voor welke acties ondernomen moeten worden in het geval zich een datalek voordoet?
De gemeente beschikt over een *Protocol afhandeling datalekken*.
Er hebben zich twee incidenten voorgedaan. Daarop is onmiddellijk actie ondernomen door de CISO en er is melding gedaan bij de Autoriteit Persoonsgegevens. Incidenten, ondernomen acties en de resultaten daarvan worden bijgehouden in de Registratie afhandeling datalekken. Bijbehorende correspondentie wordt opgeslagen in Topdesk.

9 Binnen afzienbare tijd zal een jaarlijkse verantwoording aan de raad worden gerealiseerd, vanwege de komst van de ENSIA (Eenduidige Normatiek Single Information Audit). Deze vindt plaats vanaf de tweede helft van 2017. Uit deze audit volgt een verantwoording aan de raad in het voorjaar van 2018. Een dergelijke verantwoording keert jaarlijks terug.

3. Toetsing aan het normenkader

In het voorgaande hoofdstuk hebben wij onze bevindingen verwoord en van context voorzien. In dit hoofdstuk toetsen wij de bevindingen aan het normenkader zoals vastgesteld door de Rekenkamercommissie. Dit normenkader is gebaseerd op wettelijke eisen en uitgangspunten en de voorschriften zoals die door de gemeente zelf in het lokale beleid zijn vastgelegd. Daarnaast heeft de rekenkamercommissie op basis van haar eigen visie op privacy, bepaalde normen aangescherpt. Dit betreft met name de normen waarin gevraagd wordt om een duidelijke uitwerking van procedures en werkwijzen.
Voor een korte weergave van de uitkomst van de beoordeling zijn drie kleuren ‘stoplichten’ gebruikt; rood, oranje en groen. De kleuren ‘rood’ en ‘groen’ spreken min of meer voor zich. Bij groen voldoet het beleid van de gemeente aan de gestelde norm, bij rood is dat niet het geval. Voor de kleur oranje geldt dat het beleid krap aan voldoende is, en dat er aspecten in het beleid zijn die verbetering behoeven.

Onderzoeksvragen: ***1a. Wat zijn de gemeentelijke beleidskaders rondom privacy en informatieveiligheid in het sociaal domein?***		
Norm	**Beoordeling**	**Motivatie**
In de beschrijving wordt ingegaan op: • Juridische aspecten op basis van de Wbp, AVG en de materie wetten: Suwi (en onderliggende regelgeving), Participatiewet, Wmo, Jeugdwet, Wet gemeentelijke schuldhulpverlening. • Vertaling naar de beleidskaders privacy voor het sociaal domein. • Organisatie, taken en verantwoordelijkheden in het sociaal domein. • De toepassing van informatiesystemen en ICT. • De gegevens- en informatiestromen. • De positie van en communicatie met de burger.		1. Het vastgelegde beleid concentreert zich op informatiebeveiliging. Privacybeleid wordt als onderwerp weinig uitgewerkt, hoewel in verschillende gemeentelijke stukken het perspectief van inwoners en het belang van privacybewustzijn en gedrag van medewerkers wordt onderkend als kritische factor. 2. In het Privacyprotocol voor de USD wordt een handvat met juridische onderbouwing geboden aan de uitvoeringspraktijk. 3. De taken en verantwoordelijkheden zijn duidelijk en bekend. Door de recente inpassing in de nieuwe gemeenten moeten de relaties met de CISO, concern control en de privacyjurist nog uitkristalliseren. 4. In het beleid is ruim voldoende aandacht voor de toepassing van informatiesystemen en ICT. 5. Gegevens- en informatiestromen zijn in beeld en uitgewerkt. Daarbij wordt er op gelet dat niet onnodig veel informatie wordt gedeeld. 6. De positie van en de communicatie van de burger komt aan de orde in de beleidskaders van het sociaal domein.
Onderzoeksvragen: ***1b. Hoe wordt er geanticipeerd op de AVG?***		
Norm	**Beoordeling**	**Motivatie**
De gemeente is bekend met de AVG, de impact daarvan en heeft een plan van aanpak voor de noodzakelijke aanpassingen die voor mei 2018 gerealiseerd moeten zijn.		De gemeente is bekend met de invoering van de AVG. De CISO heeft een Plan van Aanpak opgesteld met acties die moeten worden ondernomen om aan de AVG te voldoen.
Onderzoeksvragen: **1c.** ***In hoeverre voldoet het beleid aan de wettelijke grondslagen?***		
Norm	**Beoordeling**	**Motivatie**
Het beleid voldoet tenminste aan de eisen die in wet- en regelgeving worden gesteld: generiek aan de Wbp en de AVG, en specifiek voor de genoemde materiewetten.		Het Informatiebeleidsplan van de gemeente is een algemeen kader; met de aanvullingen vanuit de GAP-analyse BIG en het Plan van Aanpak AVG voldoet het aan de Wbp/AVG. Er is geen samenhangend privacyplan waarin een uitwerking is gemaakt voor de materiewetten die onder de USD vallen. Wel bevatten diverse afzonderlijke beleidsstukken wel onderdelen van een uitwerking.

Onderzoeksvraag 2. Hoe is het beleid uitgewerkt in processen?		
Norm	**Beoordeling**	**Motivatie**
In de procesbeschrijvingen en instructies sociaal domein is duidelijk welke functionaris welke gegevens in welke processtap mag verwerken, en onder welke condities dat mag		Dit is nog niet gerealiseerd, maar is wel als actie opgenomen in het Evaluatie en Verbeterplan. De analyse en het in kaart brengen van gegevensstromen, processen en hoe privacy daar aandacht in krijgt staan daarmee nog op de openstaande lijst van verbeterpunten. Daarbij verdient de omgang met (papieren) dossiers of rapportages waarin gegevens over arbeidsmogelijkheden en belastbaarheid zijn opgeslagen van cliënten Participatiewet urgente aandacht.
Onderzoeksvraag 3. Hoe is de toegang tot dossiers (autorisaties) geregeld?		
Norm	**Beoordeling**	**Motivatie**
De registraties met persoonsgegevens die in het sociaal domein worden verwerkt zijn in kaart gebracht. Het autorisatieproces voor toegang tot deze registraties staat beschreven: - er is vastgelegd: wie het besluit neemt over autorisatie (toekennen, intrekken), - er is vastgelegd wie een autorisatie inregelt, opschoont en rapporteert en hoe dat gebeurt; - er is een schema met functies-(groepen) en autorisatierollen - medewerkers; - er is een schema autorisatierollen - toegankelijke gegevens.		De CISO's hebben de belangrijkste gegevensstromen van de gemeente in kaart gebracht. Voor de USD biedt de autorisatiematrix inzicht welke functionaris/rol toegang heeft tot welke systeem en welk onderdeel daarbinnen. Het proces van autorisatie is vastgelegd in de Checklistprocedure.
Onderzoeksvraag 4. Hoe ziet het toezicht op de omgang met persoonsgegevens er uit?		
Norm	**Beoordeling**	**Motivatie**
Het toezicht op gebruik van persoons-gegevens is vastgelegd in een controleplan, waarin onder meer staat: hoe dit proces verloopt, de periodiciteit van de controles, wie daarbij betrokken zijn (functienamen en persoons-namen), wie controles uitvoert, aan wie wordt gerapporteerd, hoe de resultaten worden vastgelegd, wat de criteria zijn voor vervolgstappen, welke de vervolgstappen kunnen zijn en wie die neemt. Het controleplan sluit aan op het gemeentelijk beveiligingsplan en op het Integriteitsbeleid.		Er is een intern controleplan maar dat gaat niet in op persoonsgegevens. Een dergelijk controle(plan) is er alleen voor wat betreft de controle op raadplegen persoonsgegevens in Suwinet, zoals voorgeschreven door het normenkader Suwinet. Een controleplan dat voorziet in controle op raadplegen en verwerken persoonsgegevens door de medewerkers USD ontbreekt. Bij het opstellen van een controleplan verdient de controle op ongeoorloofd gebruik van de cliëntvolgsystemen Topicus en GWS de aandacht.

Onderzoeksvraag 5. Hoe gaat het in de praktijk, op de werkvloer?		
Norm	**Beoordeling**	**Motivatie**
De medewerkers zijn bekend met het gemeentelijk beleid bescherming persoonsgegevens, speciaal aangaande het sociaal domein. In de praktijk wordt gehandeld conform de wijze waarop de bescherming van de persoonsgegevens is geregeld in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties en de afspraken voor de verwerking van gegevens.		De medewerkers USD zijn op de hoogte van de belangrijkste punten van het gemeentelijk privacybeleid. De medewerkers USD volgen bij de uitvoering van hun de afspraken die voor USD gelden.
Onderzoeksvraag 6: In hoeverre voldoet de uitvoering aan de wettelijke normen en de onder 1 genoemde wettelijke kaders?		
Norm	**Beoordeling**	**Motivatie**
In de praktijk wordt gehandeld conform de wettelijke normen en kaders.		In de praktijk wordt gehandeld conform de wettelijke vereisten, met de kanttekening dat het informeren van de burger over zijn rechten verbetering behoeft.
Onderzoeksvraag 7: In hoeverre heeft de gemeente een balans gevonden tussen regels en procedures rondom bescherming van privacy enerzijds en een goede dienstverlening aan de burger anderzijds waarbij zij de hulp krijgen die nodig is?		
Norm	**Beoordeling**	**Motivatie**
De verwerking van persoonsgegevens staat in een goede balans tussen enerzijds procedures en anderzijds dienstverlening aan de burgers.		Medewerkers gaan vertrouwelijk om met persoonlijke informatie en wegen af welke informatie noodzakelijk is om over te dragen. Ook wordt er naar gestreefd dat cliënten niet keer op keer dezelfde of onnodige informatie hoeven te verstrekken. Vertegenwoordigers van cliëntenorganisaties zijn kritisch over de hoeveelheid informatie die cliënten geacht worden te leveren.

Onderzoeksvraag 8: Op welke manier worden medewerkers betrokken bij, en getraind in het borgen van de privacy en het versterken van informatieveiligheid?		
Norm	**Beoordeling**	**Motivatie**
De gemeente heeft vastgelegd hoe en wanneer medewerkers worden getraind in / er aandacht besteed wordt aan het onderwerp privacy.		De gemeente heeft dit niet vastgelegd. Het staat wel op de actielijst van de CISO, met de aantekening dat zij zich vooral richten op beveiligingsbeleid en minder op privacybeleid. De afdeling heeft ook niet een dergelijk instructiebeleid vastgelegd, maar zet het op de agenda indien er aanleiding is.
Onderzoeksvraag 9: Op welke manier heeft de gemeente het proces van evalueren en verbeteren ingericht?		
Norm	**Beoordeling**	**Motivatie**
De gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt.		Er is geen leer- en verbetercyclus op het gebied van privacy. In de dagelijkse praktijk is er wel aandacht voor leren- en verbeteren én zijn er plannen voor verbetermaatregelen, maar die maken geen onderdeel uit van een gestructureerde leer- en verbetercyclus.
Onderzoeksvraag 10: Is er al een evaluatie geweest en heeft dat geleid tot verbeteringen?		
Norm	**Beoordeling**	**Motivatie**
De gemeente heeft een routine voor het meten en verbeteren van de bescherming persoonsgegevens en legt vast wat de bevindingen en maatregelen zijn. Deze routine is al tenminste één keer uitgevoerd		Er bestaat bij de gemeente en bij de afdeling hiervoor geen routine.
Onderzoeksvraag 11: Wanneer en op welke manier geven burgers toestemming voor het gebruik en verwerken van gegevens?		
Norm	**Beoordeling**	**Motivatie**
De gemeente heeft vastgelegd op welke momenten, waarvoor en hoe zij burgers om toestemming vragen voor het verwerken van persoonsgegevens en geeft de burger daarover schriftelijk en mondeling informatie in begrijpelijke taal.		In de procedures (c.q. op de formulieren) is vastgelegd dat toestemming wordt gevraagd in het gesprek met de cliënt als er een aanvraag aan de orde is. De bedoeling is dat hierover mondeling informatie wordt gegeven. Volgens cliënten gebeurt dit niet altijd even duidelijk of volledig. Informatie over algemene rechten (inzage en correctie) schiet tekort. Ook schiet de schriftelijke informatie tekort, met uitzondering van de Instructie toestemming Jeugdhulp, die weer zeer uitvoering maar juridisch van aard is.
Onderzoeksvraag 12: Op welke manier worden burgers geïnformeerd over het gebruik en verwerking van hun persoonsgegevens?		
Norm	**Beoordeling**	**Motivatie**
De gemeente verschaft aan burgers schriftelijk en mondeling begrijpelijke informatie over het gebruik van hun persoonsgegevens, zowel in algemene zin als afgestemd op de verschillende fasen in het dienstverleningsproces. Daarbij wordt aangegeven met welk doel dit gebeurt, wie inzage heeft en wat er vervolgens met de gegevens gebeurt.		Algemene informatie schiet tekort. De website verwijst louter naar algemene beleidsstukken en het Privacyprotocol. Schriftelijke informatie over stapsgewijze procesuitvoering en de gegevens die daarbij aan de orde zijn is er niet.

Onderzoeksvraag 13: Op welke manier kan de gemeenteraad het beleid rondom privacy en informatieveiligheid in het sociaal domein controleren en sturen?		
Norm	**Beoordeling**	**Motivatie**
In de bestuursrapportages, programma-begroting en programmarekening wordt expliciet aandacht besteed aan de wijze waarop een correcte omgang met persoonsgegevens in het sociaal domein is gewaarborgd. Daaraan worden conclusies en maatregelen verbonden op basis van uitgevoerde controles.		In de bestuursrapportages wordt geen aandacht besteed aan privacykaders en de naleving daarvan bij de uitvoering. Noch van de gemeente in het algemeen, noch van de uitvoering in het sociaal domein.
Onderzoeksvraag 14: Op welke wijze is de gemeenteraad tot nu toe betrokken geweest?		
Norm	**Beoordeling**	**Motivatie**
Bij de ontwikkeling van het beleid voor de decentralisatie, de beleidsplannen voor de afzonderlijke beleidsterreinen in het sociaal domein, de rapportages van de Inspectie SZW over het gebruik van Suwinet en de rapportages van de AP over privacy in het sociaal domein, heeft privacy sociaal domein Gooise Meren als punt op de agenda van de Raad gestaan.		Privacy was onderdeel van de beleidsplannen rondom het sociaal domein. Verder heeft privacy niet op de agenda gestaan. Wel is eenmalig gesproken over de AVG en heeft de raad besloten de Suwi-rapportage niet te agenderen
Onderzoeksvraag 15: Is in het privacybeleid aandacht voor welke acties ondernomen moeten worden in het geval zich een datalek voordoet?		
Norm	**Beoordeling**	**Motivatie**
De gemeente heeft beleid dat betrekking heeft op de omgang met datalekken. Dit beleid voldoet aan de wettelijke vereisten.		De gemeente heeft beleid voor datalekken en heeft daarop ook al geacteerd. Dit beleid voldoet aan de wettelijke normen.

4. Conclusies en aanbevelingen

4.1 Samenvatting en oordeel

Algemeen beeld
Uit het onderzoek is duidelijk geworden dat de gemeente Gooise Meren informatiebeveiliging en het beschermen van de privacy van de inwoners voortvarend ter hand heeft genomen. Het beleid doet recht aan wettelijke eisen en richtlijnen. De verdere uitwerking heeft de aandacht.

Er is een privacyprotocol en medewerkers van de gemeente zijn bekend met de regels en zeggen daar naar te handelen. Kwaliteitsmedewerkers binnen het sociaal domein letten er op dat medewerkers niet meer informatie in een dossier opnemen dan strikt noodzakelijk is voor de dienstverlening. Ook heeft de gemeente er voor gezorgd dat de persoonlijke gegevens van inwoners alleen toegankelijk zijn voor medewerkers die deze informatie nodig hebben om hun werk uit te voeren. De procedures voor deze autorisaties zijn op orde.

Het onderzoek heeft ook een aantal verbeterpunten in beeld gebracht. Vertegenwoordigers van cliëntenorganisaties hebben vragen én zorgen bij het privacybeleid. Vooralsnog worden zij in dit verband te weinig gerust gesteld door het beleid en de voorlichting daarover. Ook wordt het privacybeleid en de uitvoering daarvan niet structureel geëvalueerd en wordt daarover geen verantwoording afgelegd aan de gemeenteraad.

Beleid en uitvoering
Binnen de gemeente Gooise Meren bestaat er veel aandacht voor informatiebeveiliging. In dat verband zijn ook verschillende aspecten van het privacybeleid via systemen, procedures en applicaties ingeregeld. Er zijn Chief Information Officers (CISO's) aangesteld, die nu als belangrijke taak hebben om in de relatief jonge gemeente de basis van de informatiehuishouding en -beveiliging op orde te krijgen. Over het geheel genomen wordt recht gedaan aan wettelijke basisvereisten met betrekking tot privacy.

Naar mening van direct betrokkenen in de gemeentelijke organisatie is de basis dusdanig stevig ingericht dat er in de dagelijkse uitvoeringspraktijk geen bijzondere aandacht hoeft te worden besteed aan het realiseren van waarborgen voor de privacy van de cliënten. Bij de inrichting van het sociale domein heeft dit immers al afdoende plaatsgevonden. Nieuwe medewerkers worden bij het inwerken vertrouwd gemaakt met zowel het belang van het waarborgen van de privacy als de gemaakte afspraken en geldende procedures. Indien binnen de organisatie naar mening van betrokkenen onnodig veel informatie wordt gedeeld, spreken medewerkers elkaar hier op aan. Dit gebeurt op ad hoc basis. Het beleid zou echter meer structureel in het dagelijks handelen van de medewerkers kunnen worden verankerd.

Aan de raad wordt geen verslag uitgebracht over de stand van zaken en de ontwikkelingen rond het privacybeleid. Het beleid, de naleving en verbeteracties zouden meer aandacht van de raad kunnen krijgen en onderwerp in bestuursrapportages kunnen zijn.

Organisatie en bedrijfsvoering
De relatief jonge gemeente Gooise Meren is nog steeds druk bezig met het inregelen van verschillende procedures, afspraken en functies. Bij de inrichting van het beleid is gebruik gemaakt van de expertise van de jurist die werkzaam is bij de Regio Gooi- en Vechtstreek. Formeel is dat momenteel niet meer mogelijk. Het is de vraag of een dergelijke juridische functie nog steeds nodig is om de vertaling te maken van regelgeving naar praktijk. Deze vraag is vooralsnog niet expliciet aan de orde gesteld binnen de gemeente, waardoor het voor sommige medewerkers niet duidelijk is tot wie zij zich met specifieke juridische vragen met betrekking tot privacy kunnen wenden.
Verder bestaat er nog geen duidelijkheid over de FG (Functionaris Gegevensbeheer). Deze functie moet krachtens de AVG in mei 2018 ingevuld zijn .
Eveneens kan worden opgemerkt dat de functie en de verantwoordelijkheden van de CISO's nog niet zijn uitgekristalliseerd en dat de gemeente nog niet voldoet aan alle vereisten van de Baseline Informatiebeveiliging Gemeenten.

Cliëntenperspectief
Uit het onderzoek is naar voren gekomen dat er geen sprake is van acute of urgente problemen of tekortkomingen als het gaat om het waarborgen van de privacy van cliënten. Tegelijkertijd is wel gebleken dat vertegenwoordigers van cliëntenorganisaties vragen én zorgen hebben bij het privacybeleid. Vooralsnog worden zij in dit verband te weinig gerust gesteld door de gemeentelijke organisatie. In de voorlichting heeft de gemeente te weinig aandacht voor het perspectief van de cliënten en de aldaar bestaande zorgen.

4.2 Aanbevelingen

De basis is op orde en de verdere uitwerking krijgt de aandacht. Vanuit de verbeterpunten zijn er vier belangrijke aanbevelingen te doen rondom privacy in het sociaal domein.[10]

1. **Ga in gesprek met cliënten** - Ga in gesprek met cliënten en burgers om een goed beeld te krijgen van hun ervaringen, vragen en zorgen rond privacy en ga na wat de gemeente kan doen om daar op een goede manier mee om te gaan. Neem hiervoor de rapporten van Samenkracht! als basis.
2. **Verbeter de voorlichting** - Verbeter de gemeentelijke voorlichting over privacy in het sociaal domein. Neem cliënten als uitgangspunt en bedenk waar, wanneer en op welke manier zij het beste geïnformeerd kunnen worden. Pas in ieder geval de website aan en maak folders die mensen thuis nog eens na kunnen lezen. Zorg dat de informatie voor iedereen toegankelijk en begrijpelijk is.[11]
3. **Houd privacy levend in de organisatie!** - Houd privacy hoog op de agenda bij medewerkers en maak een plan om dat *gestructureerd* te doen. Op dit onderwerp mag de aandacht niet verslappen. Dat kan bijvoorbeeld door het onderwerp met enige regelmaat te agenderen in werkoverleggen en daar casussen en 'lastige situaties' te bespreken. Of door geplande organisatiebrede opfrisacties. Het is belangrijk dat medewerkers *automatisch* aan het onderwerp toekomen en dat zij zo ruimte krijgen om hun professionele aanpak te borgen. Zorg dat privacy leeft! Ook een volgroeide boom heeft aandacht nodig.

[10] In bijlage E is uitgewerkt hoe de aanbevelingen en aandachtspunten samenhangen met de bevindingen van dit onderzoek.
[11] Er zijn goede voorbeelden te vinden bij de Vereniging Nederlandse Gemeenten en de Landelijke Cliëntenraad. Ook kan kennisgenomen worden van de manier waarop de gemeente Amsterdam dit onderwerp samen met cliënten en een adviesraad met specialisten heeft opgepakt. Bij commerciële bedrijven (zoals bol.com, Coolblue of WeTransfer) zijn interessante voorbeelden te vinden van hoe moeilijk en juridisch getint jargon toegankelijk kan worden verwoord.

4. **En laat zien wat je doet** – Open de black box van privacy in het sociaal domein en laat zien wat je als gemeente deed, doet en van plan bent om de privacy te waarborgen. Geef daarbij expliciet aandacht aan hoe medewerkers in staat worden gesteld om bekwaam te opereren. Leg daarover verantwoording af aan de gemeenteraad. (Dus raadsleden: vraag hier om). Zo toon je je professionaliteit naar buiten toe en bouw je aan vertrouwen bij burgers en bij samenwerkingspartners in het sociaal domein.

4.3 Verdere aandachtspunten

Veel in beweging dus voer het gesprek

Naast de vier belangrijke algemene aanbevelingen, zijn er door nieuwe AVG en door veranderingen bij de USD, voldoende aanleidingen om het onderwerp privacy op korte termijn te agenderen in de raad en het gesprek te voeren over de toekomstige eisen die aan het beleid zullen worden gesteld en de keuzen die de gemeente, en daarmee uiteindelijk de raad, daarin wil maken.

Toepassing van de AVG

De komende tijd zal de toepassing van de AVG nog veel aandacht vragen. De gemeente zal een Functionaris Gegevensbescherming aanstellen die in afstemming met de CISO's de vraagstukken rondom privacy kan oppakken. Daar hoort ook bij dat de werkwijzen en procedures van de gemeente nog in concrete werkinstructies gegoten moeten worden. Uit het onderzoek blijkt dat twee vragen daarbij extra aandacht verdienen. (1) Wat zijn de afspraken rondom de gezondheidsgegevens van cliënten Participatiewet? (2) En hoe vaak en hoe wil de organisatie steekproefsgewijs controles uitvoeren op loggings op Topicus en GWS?

Herontwerp processen USD

Bij de USD blijft het onderwerp zeker nog een rol spelen. De organisatie wil de processen opnieuw inrichten waarbij enkelvoudige vragen direct door een specialist behandeld worden en niet meer eerst door een vraagverhelderaar worden uitgediept. Bij dat herontwerp komen privacyvraagstukken vanzelf weer boven drijven. Medewerkers én cliënten kunnen daar in meedenken. Dat helpt om het privacybewustzijn te verhogen en privacy te borgen in de nieuwe processen. Een nieuwe PIA sluit het herontwerp op een goede manier af.

Losse vraagstukken

Tot slot ligt er nog een aantal vragen rondom privacy voor de organisatie die aandacht behoeven. Is er naast de kwaliteitsmedewerker en de abonnementen op landelijke kennisbanen, ook behoefte aan een juridisch medewerker die vragen kan oppakken rondom privacy? En wat hebben medewerkers nodig om op hun nieuwe open (maar ook gehorige) flexplekken in het gemeentehuis zorgvuldig met persoonlijke gegevens te kunnen werken? Ook deze vragen dienen nog door de gemeentelijke organisatie opgepakt en beantwoord te worden.

Bijlage A Lijst van gebruikte afkortingen

Afkorting	Betekenis
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BIG	Baseline Informatiebeveiliging Gemeenten
CISO	Chief Information Security Officer
FG	Functionaris Gegevensbescherming
PIA	Privacy Impact Assessment
RGV	Regio Gooi- en Vechtstreek
USD	Uitvoeringsorganisatie Sociaal Domein Gooise Meren
Wbp	Wet bescherming persoonsgegevens
Wmo	Wet maatschappelijke ondersteuning

Bijlage B Geïnterviewde personen

Gemeente Gooise Meren	
J. Franx,	Wethouder voor o.a. Financiën, ICT en P&O
P. Lensselink	Afdelingshoofd/strategisch manager sociaal domein,
T. van Putten	Adjunct afdelingshoofd/strategisch manager sociaal domein
I. Rigters	Chief Information Security Officer
P. Stove	Chief Information Security Officer
N. Langley	Specialist Jeugdwet
L. Vos	Consulent Jeugdwet
J. van Kessel	Consulent Wmo
R. Waldrom	Kwaliteitsmedewerker Sociaal domein
L. van Elswijk	Specialist schuldhulpverlening
J. Klompstra	Specialist inkomen
W. de Bruin,	Applicatiebeheerder Sociaal Domein
H. van der Heiden	(Voormalig) beleidsmedewerker Samenkracht!
L. Achouiti,	Medewerker administratie Sociaal Domein
S. Pasman	Controller
T. van Veen	Werkconsulent van de afdeling Sociaal Domein,
Regio Gooi- en Vechtstreek	
W. van Neer	Inkoop en contractmanager
M. van der Spek-Stikkelorum	Medewerker inkoop en contractmanagement,
R. Colpaart	Senior contractbeheerder / verantwoordelijk voor digitaal leefplein,
M. Vinke	Juridisch adviseur
Overig	
P. Vomberg	Lid van de Wmo-raad
L. Mast, C. Grois en R. Bosboom,	Leden van de Adviesraad Werk en Inkomen
F. Liefferink	Directeur bedrijfsvoering GGZ Centraal Fornhese
H. Schouten	Medewerker Kind, Jongere en Gezin, Sherpa

Bijlage C Bestudeerde documentatie

Detailstructuur Gooise Meren. Maart 2016.
Informatiebeveiligingsbeleid Gooise Meren. Beleidsstuk. Dec. 2016
I&A-plan Gooise Meren. Meer met minder. Oktober 2016
Presentatie voortgang GAP analyse Gooise Meren. 27 maart 2017
Protocol afhandeling datalekken. Dec. 2016
Regeling ambtelijke integriteit en gedragscode 2016.
10 Gouden Regels.
Aanpak invoering AVG in de gemeente Gooise Meren. Juli 2016.
Accountantsverslag over 2016. Juni 2017
Nota informatiebeveiligingsbeleid Wijzer 2015
Informatiebeveiligingsplan Wijzer 2015
Verbeterplan en evaluatie informatiebeveiligingsplan Wijzer/USD. Maart 2017
Privacyprotocol Sociaal Domein. Mei 2015
Keuzenota. Voorstellen regie en privacy sociaal domein. Regio GV. Juni 2016
Voorbeeld Inkoopdocument Toelating. Regio GV. 2016.
Implementatieplannen Jeugd. Plan van Aanpak. Sept. 2016.
Procesregie Wijzer: werkwijze, systemen, achtergrond. (Handleiding complexe casussen). Aug. 2016
Proces integrale toegang USD.
Protocol huisbezoeken. 2013
Autorisatiestructuur USD/Wijzer
Inwerkprogramma Wijzer.
Intern controleplan Wijzer. Sept. 2016
Weekberichten (intern) Wijzer.
Implementatie plannen jeugd. September 2016
Bevindingen Jeugd en Wmo interne controle eerste en tweede kwartaal 2015
Rapport Inspectie SZW over gebruik Suwinet in 2015. Jan. 2016
Rapportage Halfjaarlijkse controle Suwinet: eerste half jaar 2016.
Procedure veilig gebruik en beheer Suwinet. April 2016
Grondslagen verwerking persoonsgegevens sociaal domein. Regio GV. Maart 2017.
Samenkracht: cliëntperspectief op gemeentelijke dienstverlening 2013-2016
Verslag Samenkracht werkbijeenkomst Privacy 9 dec. 2015
Samenkracht: cliëntperspectief op gemeentelijke dienstverlening. Format terugkoppeling, Jan. 2017
Informatie voor burgers:
Folder Wijzer: Algemene informatie
Folder Wijzer: Het gesprek.
Nieuwsbrief Wijzer, sept. 2015 over beveiliging persoonsgegevens
Nieuwsbrief Wijzer, maart 2017 over Zivver
Wijzer: Toestemmingsverklaring Jeugdhulp plus instructie 2016
Toestemmingsverklaring schuldhulpverlening
Wijzer: Toestemmingsverklaring Wmo
Website gemeente GM

Bijlage D Gehanteerd normenkader

	Onderzoeksvraag	Norm
Beleid		
1	*Wat zijn de gemeentelijke beleidskaders rondom privacy en informatieveiligheid in het sociaal domein?* *Hoe wordt er geanticipeerd op de AVG?* *In hoeverre voldoet het beleid aan de wettelijke grondslagen?*	In de beschrijving wordt ingegaan op: • Juridische aspecten op basis van de Wbp, AVG en de materie wetten: Suwi (en onderliggende regelgeving), Participatiewet, Wmo, Jeugdwet, Wet gemeentelijke schuldhulpverlening. • Vertaling naar de beleidskaders privacy voor het sociaal domein. • Organisatie, taken en verantwoordelijkheden in het sociaal domein. • De toepassing van informatiesystemen en ICT. • De gegevens- en informatiestromen. • De positie van en communicatie met de burger. De gemeente is bekend met de AVG, de impact daarvan en heeft een plan van aanpak voor de noodzakelijke aanpassingen die voor mei 2018 gerealiseerd moeten zijn. Het beleid voldoet tenminste aan de eisen die in wet- en regelgeving worden gesteld: generiek aan de Wbp en de AVG, en specifiek voor de genoemde materiewetten.
2	*Hoe is het beleid uitgewerkt en geborgd in processen?*	In de procesbeschrijvingen en instructies sociaal domein is duidelijk welke functionaris welke gegevens in welke processtap mag verwerken, en onder welke condities dat mag.
3	*Hoe is de toegang tot dossiers (autorisaties) geregeld?*	De registraties met persoonsgegevens die in het sociaal domein worden verwerkt zijn in kaart gebracht. Het autorisatieproces voor toegang tot deze registraties staat beschreven: - er is vastgelegd: wie het besluit neemt over autorisatie (toekennen, intrekken), - er is vastgelegd wie een autorisatie inregelt, opschoont en rapporteert en hoe dat gebeurt; - er is een schema met functies-(groepen) en autorisatierollen - medewerkers; - er is een schema autorisatierollen - toegankelijke gegevens.
4	*Hoe ziet het toezicht op de omgang met de persoonsgegevens er uit?*	Het toezicht op gebruik van persoonsgegevens is vastgelegd in een controleplan, waarin onder meer staat: hoe dit proces verloopt, de periodiciteit van de controles, wie daarbij betrokken zijn (functienamen en persoonsnamen), wie controles uitvoert, aan wie wordt gerapporteerd, hoe de resultaten worden vastgelegd, wat de criteria zijn voor vervolgstappen, welke de vervolgstappen kunnen zijn en wie die neemt. Het controleplan sluit aan op het gemeentelijk beveiligingsplan en op het Integriteitsbeleid.
5	*Hoe gaat het in de praktijk, op de werkvloer?*	De medewerkers zijn bekend met het gemeentelijk beleid bescherming persoonsgegevens, speciaal aangaande het sociaal domein. **In de praktijk wordt gehandeld conform de wijze waarop de bescherming van de persoonsgegevens is geregeld in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties en de afspraken voor de verwerking van gegevens.**

	Onderzoeksvraag	Norm
6	*In hoeverre voldoet de uitvoering aan de wettelijke normen en de onder 1 genoemde wettelijke kaders?*	In de praktijk wordt gehandeld conform de wettelijke normen en kaders.
7	*In hoeverre heeft de gemeente een balans gevonden tussen regels en procedures rondom de bescherming van privacy enerzijds en een goede dienstverlening aan de burger anderzijds waarbij zij de hulp krijgen die nodig is?*	De verwerking van persoonsgegevens staat in een goede balans tussen enerzijds procedures en anderzijds dienstverlening aan de burgers.
Leren en Verbeteren		
8	*Op welke manier worden medewerkers betrokken bij, en getraind in het borgen van de privacy en het versterken van de informatieveiligheid?*	De gemeente heeft vastgelegd hoe en wanneer medewerkers worden getraind in / er aandacht besteed wordt aan het onderwerp privacy.
9	*Op welke manier heeft de gemeente het proces van evalueren en verbeteren ingericht?*	De gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt.
10	*Is er al een evaluatie geweest en hoeverre heeft dat tot verbeteringen geleid?*	De gemeente heeft een routine voor het meten en verbeteren van de bescherming persoonsgegevens en legt vast wat de bevindingen en maatregelen zijn. Deze routine is al tenminste één keer uitgevoerd
Positie burger		
11	*Wanneer en op welke manier geven burgers toestemming voor het gebruik en verwerken van gegevens?*	De gemeente heeft vastgelegd op welke momenten, waarvoor en hoe zij burgers om toestemming vragen voor het verwerken van persoonsgegevens en geeft de burger daarover schriftelijk en mondeling informatie in begrijpelijke taal.
12	*Op welke manier worden burgers geïnformeerd over het gebruik en de verwerking van hun persoonsgegevens?*	De gemeente verschaft aan burgers schriftelijk en mondeling begrijpelijke informatie over het gebruik van hun persoonsgegevens, zowel in algemene zin als afgestemd op de verschillende fasen in het dienstverleningsproces. Daarbij wordt aangegeven met welk doel dit gebeurt, wie inzage heeft en wat er vervolgens met de gegevens gebeurt.
Kaderstellende en controlerende taak gemeenteraad		
13	*Op welke manier kan de gemeenteraad het beleid rondom privacy en informatieveiligheid in het sociaal domein controleren en sturen?*	In de bestuursrapportages, programmabegroting en programmarekening wordt expliciet aandacht besteed aan de wijze waarop een correcte omgang met persoonsgegevens in het sociaal domein is gewaarborgd. Daaraan worden conclusies en maatregelen verbonden op basis van uitgevoerde controles.
14	*Op welke wijze is de raad tot nu toe betrokken geweest?*	Bij de ontwikkeling van het beleid voor de decentralisatie, de beleidsplannen voor de afzonderlijke beleidsterreinen in het sociaal domein, de rapportages van de Inspectie SZW over het gebruik van Suwinet en de rapportages van de AP over privacy in het sociaal domein, heeft privacy sociaal domein Gooise Meren als punt op de agenda van de Raad gestaan.
15	*Is er in het privacybeleid van de gemeente aandacht voor welke acties ondernomen moeten worden in het geval zich een datalek voordoet?*	De gemeente heeft beleid dat betrekking heeft op de omgang met datalekken. Dit beleid voldoet aan de wettelijke vereisten.

Bijlage E Van beoordeling naar aanbeveling

Onderzoeksvraag 2. Hoe is het beleid uitgewerkt in processen?		
Beoordeling	**Motivatie**	**Aanbeveling / aandachtspunt**
	Dit is nog niet gerealiseerd, maar is wel als actie opgenomen in het Evaluatie en Verbeterplan. De analyse en het in kaart brengen van gegevensstromen, processen en hoe privacy daar aandacht in krijgt staan daarmee nog op de openstaande lijst van verbeterpunten. Daarbij verdient de omgang met (papieren) dossiers of rapportages waarin gegevens over arbeidsmogelijkheden en belastbaarheid zijn opgeslagen van cliënten Participatiewet urgente aandacht.	Zie de verdere aandachtspunten onder 'toepassing van de AVG'
Onderzoeksvraag 4. Hoe ziet het toezicht op de omgang met persoonsgegevens er uit?		
Beoordeling	**Motivatie**	**Aanbeveling / aandachtspunt**
	Er is een intern controleplan maar dat gaat niet in op persoonsgegevens. Een dergelijk controle(plan) is er alleen voor wat betreft de controle op raadplegen persoonsgegevens in Suwinet, zoals voorgeschreven door het normenkader Suwinet. Een controleplan dat voorziet in controle op raadplegen en verwerken persoonsgegevens door de medewerkers USD ontbreekt. Bij het opstellen van een controleplan verdient de controle op ongeoorloofd gebruik van de cliëntvolgsystemen Topicus en GWS de aandacht.	Zie de verdere aandachtspunten onder 'toepassing van de AVG'
Onderzoeksvraag 7: In hoeverre heeft de gemeente een balans gevonden tussen regels en procedures rondom bescherming van privacy enerzijds en een goede dienstverlening aan de burger anderzijds waarbij zij de hulp krijgen die nodig is?		
Beoordeling	**Motivatie**	**Aanbeveling / aandachtspunt**
	Medewerkers gaan vertrouwelijk om met persoonlijke informatie en wegen af welke informatie noodzakelijk is om over te dragen. Ook wordt er naar gestreefd dat cliënten niet keer op keer dezelfde of onnodige informatie hoeven te verstrekken. Vertegenwoordigers van cliëntenorganisaties zijn kritisch over de hoeveelheid informatie die cliënten geacht worden te leveren.	Ga in gesprek met cliënten. Zie ook de verdere aandachtspunten onder 'herontwerp processen USD
Onderzoeksvraag 8: Op welke manier worden medewerkers betrokken bij, en getraind in het borgen van de privacy en het versterken van informatieveiligheid?		
Beoordeling	**Motivatie**	**Aanbeveling / aandachtspunt**
	De gemeente heeft dit niet vastgelegd. Het staat wel op de actielijst van de CISO, met de aantekening dat zij zich vooral richten op beveiligingsbeleid en minder op privacybeleid. De afdeling heeft ook niet een dergelijk instructiebeleid vastgelegd, maar zet het op de agenda indien er aanleiding is.	Houd privacy levend in de organisatie.
Onderzoeksvraag 9: Op welke manier heeft de gemeente het proces van evalueren en verbeteren ingericht?		
Beoordeling	**Motivatie**	**Aanbeveling / aandachtspunt**
	Er is geen leer- en verbetercyclus op het gebied van privacy. In de dagelijkse praktijk is er wel aandacht voor leren- en verbeteren én zijn er plannen voor verbetermaatregelen, maar die	Houd privacy levend in de organisatie. En laat zien wat je doet

	maken geen onderdeel uit van een gestructureerde leer- en verbetercyclus.	
Onderzoeksvraag 10: Is er al een evaluatie geweest en heeft dat geleid tot verbeteringen?		
Beoordeling	**Motivatie**	**Aanbeveling / aandachtspunt**
	Er bestaat bij de gemeente en bij de afdeling hiervoor geen routine.	Houd privacy levend in de organisatie. En laat zien wat je doet!
Onderzoeksvraag 11: Wanneer en op welke manier geven burgers toestemming voor het gebruik en verwerken van gegevens?		
Beoordeling	**Motivatie**	
	In de procedures (c.q. op de formulieren) is vastgelegd dat toestemming wordt gevraagd in het gesprek met de cliënt als er een aanvraag aan de orde is. De bedoeling is dat hierover mondeling informatie wordt gegeven. Volgens cliënten gebeurt dit niet altijd even duidelijk of volledig. Informatie over algemene rechten (inzage en correctie) schiet tekort. Ook schiet de schriftelijke informatie tekort, met uitzondering van de Instructie toestemming Jeugdhulp, die weer zeer uitvoering maar juridisch van aard is.	Ga in gesprek met cliënten Verbeter de voorlichting
Onderzoeksvraag 12: Op welke manier worden burgers geïnformeerd over het gebruik en verwerking van hun persoonsgegevens?		
Beoordeling	**Motivatie**	
	Algemene informatie schiet tekort. De website verwijst louter naar algemene beleidsstukken en het Privacyprotocol. Schriftelijke informatie over stapsgewijze procesuitvoering en de gegevens die daarbij aan de orde zijn is er niet.	Ga in gesprek met cliënten Verbeter de voorlichting
Onderzoeksvraag 13: Op welke manier kan de gemeenteraad het beleid rondom privacy en informatieveiligheid in het sociaal domein controleren en sturen?		
Beoordeling	**Motivatie**	
	Privacy was onderdeel van de beleidsplannen rondom het sociaal domein. Verder heeft privacy niet op de agenda gestaan. Wel is eenmalig gesproken over de AVG en heeft de raad besloten de Suwi-rapportage niet te agenderen	Houd privacy levend in de organisatie. En laat zien wat je doet Zie ook de verdere aandachtspunten onder ‘veel in beweging dus voer het gesprek’.
Onderzoeksvraag 14: Op welke wijze is de gemeenteraad tot nu toe betrokken geweest?		
Beoordeling	**Motivatie**	
	Naar aanleiding van deze punten heeft privacy niet op de agenda gestaan. Wel is eenmalig gesproken over de AVG.	Laat privacy leven in de organisatie. En laat zien wat je doet! Zie ook de verdere aandachtspunten onder ‘veel in beweging dus voer het gesprek’.

Bijlage F Privacyprotocol 2015 en de Tien Gouden Regels

Privacy Protocol Sociaal Domein

Inleiding

De gemeenten Naarden, Muiden en Bussum willen integrale en effectieve ondersteuning bieden aan haar inwoners bij vragen en problemen op het gebied van zorg, welzijn en inkomen. Ondersteuning die aanvullend is op de eigen mogelijkheden van de inwoner en zijn (of haar) sociale netwerk. Ondersteuning als inwoners zichzelf melden, maar ook proactief op basis van signalen dat ondersteuning noodzakelijk en gewenst is.

Om dit mogelijk te maken moeten wij persoonsgegevens verwerken en uitwisselen met partners in de regio, zoals instellingen voor thuiszorg of jeugdzorg. Dat willen we rechtmatig en zorgvuldig doen. We willen transparant en duidelijk zijn hoe we omgaan met de privacy van onze inwoners en betrokkenen. In dit protocol is uitgewerkt hoe wij dit doen. Het protocol bevat algemene regels, geen antwoord op elke vraag. Het antwoord is namelijk sterk afhankelijk van een zorgvuldige afweging van belangen die per situatie kan verschillen.

Dit protocol is opgesteld binnen de context van het sociaal domein waarin, op basis van wet- en regelgeving (zie hiervoor de bijlage: Van toepassing zijnde wet- en regelgeving), er duidelijke kaders zijn voor het omgaan met privacy. Het vormt geen zelfstandige grondslag voor gegevensuitwisseling en –verwerking. Het protocol is bedoeld als leesbare uitwerking van deze regels voor inwoners, medewerkers en anderen. En moet leiden tot een eenduidige werkwijze voor het verwerken van gegevens voor alle gemeenten in de regio.

Belangrijke begrippen

Betrokkene	de (natuurlijke) persoon op wie een persoonsgegeven betrekking heeft.
Bestand	een gestructureerde verzameling persoonsgegevens, die volgens bepaalde criteria toegankelijk is;
Bewerker	een partij die in opdracht persoonsgegevens verwerkt, maar die niet direct onder de verantwoordelijkheid/ aansturing van de gemeente Naarden, Muiden of Bussum valt;
Bijzondere persoonsgegevens	persoonsgegevens over religie/ levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele geaardheid, lidmaatschap van een vakvereniging, strafrechtelijke gegevens, persoonsgegevens over hinderlijk/ onrechtmatig gedrag in verband met een opgelegd verbod;
Persoonsgegevens	alle gegevens die betrekking hebben op een geïdentificeerde of een identificeerbare natuurlijke persoon (betrokkene);
Verantwoordelijke	degene die (binnen de eindverantwoordelijkheid van het college) de uitvoerende verantwoordelijkheid heeft voor het beheer van persoonsgegevens. Dit is voor het Sociaal Domein het afdelingshoofd;
Verwerking van persoonsgegevens	elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, verspreiden, samenbrengen, met elkaar in verband brengen, afschermen, wissen of vernietigen;
Verwijzer	een beroepskracht die op basis van contacten met een inwoner een behoefte aan ondersteuning ziet en de inwoner aanmeldt.
Wijzer	Uitvoeringsdienst Sociaal Domein voor de gemeenten Naarden, Muiden en Bussum

Doel van de gegevensverwerking

Doel van de gegevensverwerking binnen het Sociaal Domein is het bieden van ondersteuning aan inwoners van onze gemeenten bij vragen of behoeften op het gebied van zorg, welzijn en inkomen, aansluitend op de mogelijkheden waarover zijzelf en hun sociale netwerk beschikken.

Om dit doel te bereiken moeten wij persoonsgegevens verwerken, waaronder ook *bijzondere persoonsgegevens* (namelijk strafrechtelijke gegevens en gezondheidsgegevens), passend bij het doel van de gegevensverwerking, dus in termen van het effect op de benodigde ondersteuning, waarbij niet meer wordt vastgelegd dan noodzakelijk!

In brede zin omvat de verwerking ook het evalueren van de ondersteuning en het voldoen aan verplichtingen ten aanzien van (financiële) verantwoording en beleidsontwikkeling/ onderzoek. Maar in deze gevallen (met uitzondering van onderzoek naar een individuele persoon) worden de gegevens bewerkt zodat deze niet te herleiden zijn naar geïdentificeerde / te identificeren personen.

Toepassingsgebied

Dit protocol is van toepassing op de verwerking van persoonsgegevens binnen het Sociaal Domein (zorg, welzijn en inkomen), niet op de verstrekking van gegevens *aan* de gemeente door andere partijen (zorgaanbieders, scholen of 'Veilig Thuis'). Welke informatie zij mogen verstrekken wordt bepaald door de privacywetgeving waaronder de betreffende partij valt en hun eigen privacyregelingen.

Verantwoordelijkheden van management en medewerkers

Alle medewerkers van Wijzer en alle ingehuurde medewerkers hebben een integriteitsverklaring getekend, waarin het omgaan met vertrouwelijke gegevens (zoals plicht tot geheimhouding) is vastgelegd. Iedereen die (binnen het doel van de gegevensbewerking) bevoegd is om persoonsgegevens te bewerken zorgt ervoor dat:

- deze gegevens rechtmatig verkregen zijn en juist, volledig en ter zake zijn;
- er afdoende maatregelen genomen zijn om deze gegevens te beveiligen;
- verwerking gebeurt conform dit protocol en ontvangen instructies over beveiliging van persoonsgegevens.

De hoofdregels voor zorgvuldig omgaan met privacy

1. de verwerking van persoonsgegevens moet passen binnen het doel waarvoor deze verstrekt zijn. Er mogen niet méér persoonsgegevens verwerkt worden dan noodzakelijk;
2. elke betrokkene heeft recht om te weten wat er over hem is vastgelegd. Het recht op inzage (en afschrift, correctie of vernietiging) beperkt zich tot de *eigen gegevens*;
3. het opvragen van of verstrekken van gegevens aan derden gebeurt op basis van een *wettelijke grond* of op basis van *bewuste toestemming van de betrokkene* als deze ontbreekt. Als de noodzakelijke hulpverlening niet op gang kan komen omdat de noodzakelijke toestemming geweigerd wordt kan in bepaalde gevallen worden afgeweken van deze regel.

De hoofdregels zijn redelijk overzichtelijk en duidelijk, de werkelijkheid is weerbarstiger. Hoe complexer een zaak, hoe meer de afweging gemaakt moet worden tussen het verwerken van extra persoonsgegevens versus de noodzaak voor ondersteuning.
De behandelend ambtenaar moet zich continu afvragen: is het noodzakelijk voor gestelde doel, is er een wettelijke grondslag, kan het ook met minder/ anders, is het nog proportioneel, zijn er beperkingen of specifieke regels, is er sprake van een vitaal belang of is de veiligheid van betrokkene of anderen in gevaar?

Informeren en het vragen van toestemming

Binnen het Sociaal Domein wordt een heel scala aan vragen en aanvragen behandeld, van eenvoudig tot en met 'multiprobleem gezinnen' met een complexe problematiek. *Voor veel taken is er een wettelijke basis voor het verwerken van gegevens*, en over het algemeen is het verband tussen de benodigde gegevens en het doel bij deze zaken duidelijk zichtbaar. Denk aan het aanvragen van een uitkering of een rolstoel. Wij gaan ervan uit dat dit duidelijk is voor de betrokkene, en dat toelichting op de gegevensverwerking niet noodzakelijk is tenzij de betrokkene hier behoefte aan heeft.

Bij zaken waarbij wij vermoeden dat de relatie tussen doel en gegevens voor de betrokkene minder duidelijk is, en/of waar toestemming voor verwerking noodzakelijk is, wordt de betrokkene *zo spoedig mogelijk (waar mogelijk vooraf) geïnformeerd*:

- Met welk doel de gegevens worden verwerkt;

- Indien van toepassing, welke verwijzer de betrokkene aangemeld heeft en welke gegevens deze heeft verstrekt;
- Bij wie welke gegevens opgevraagd gaan worden en aan wie welke gegevens verstrekt worden om de benodigde ondersteuning te kunnen leveren;
- Welke rechten de inwoner heeft als het gaat om de verwerking van zijn gegevens en hoe deze rechten uit te oefenen.

Als *toestemming voor het verwerken van gegevens noodzakelijk* is dan wordt de cliënt zo vroeg mogelijk in het traject om toestemming gevraagd, maar vóórdat er gegevens worden opgevraagd bij of verstrekt aan derden. De gegeven toestemming wordt vastgelegd in het dossier. De medewerker maakt de afweging of vastlegging middels een aantekening in het dossier volstaat of dat, gezien de belangen/ risico's, er een *toestemmingsformulier* getekend moet worden.

Verwijzing en (anonieme) signalen

Als gemeente ontvangen wij verwijzingen en signalen over een behoefte aan ondersteuning. Deze signalen en verwijzingen kunnen zowel via professionele verwijzers (zoals artsen) binnenkomen als via (al dan niet anonieme) inwoners. Wij gaan er bij professionele verwijzers van uit dat zij, vanuit hun professionaliteit en hun eigen privacy regels, vooraf de betrokkene hebben geïnformeerd en toestemming hebben gevraagd voor aanmelding en het verstrekken van gegevens. Dit wordt bij voorkeur schriftelijk vastgelegd.
Als er geen toestemming wordt gegeven of kan worden gegeven maar er is wel een dringende noodzaak (vitaal belang) dan zal een professionele verwijzer vanuit een wettelijke plicht alsnog een signaal afgeven.

Bij professionele verwijzers informeren wij de betrokkene over wie de aanmelding gedaan heeft en welke gegevens verstrekt zijn. Bij signalen van anderen (al dan niet anoniem) vermelden wij de naam alleen met toestemming van de melder. Zowel aanmeldingen als signalen *bespreken wij met de betrokkene vóór verdere verwerking*, tenzij er aanwijzingen zijn dat de veiligheid van betrokkene, gezin of anderen wordt bedreigd.

Toegang tot persoonsgegevens in het bestand

De persoonsgegevens in het bestand zijn afgeschermd op basis van autorisaties: enkel voor degenen die de ondersteuning (passend binnen het doel) moeten kunnen leveren, de direct leidinggevenden en degenen die belast zijn met de afhandeling van bezwaren en klachten over de geboden ondersteuning. Lees- en schrijfrechten (opnemen in bestand, aanvullen, wijzigen) zijn vastgelegd, passend bij de rol. Daarnaast wordt toegang gegeven als een wettelijke plicht daartoe noodzaakt.

Verstrekken van persoonsgegevens aan derden

Onder *'derden'* rekenen we in dit document alle partijen buiten de betrokkene en degenen die in opdracht van Wijzer gegevens verwerken (hetzij onder rechtstreeks gezag of als bewerker op basis van een bewerkingsovereenkomst) en die *ontvanger* van persoonsgegevens zijn. Bij de verstrekking aan derden wordt *toestemming van de betrokkene* gevraagd (zie 'informeren en het vragen van toestemming') als een wettelijke grond voor het delen van informatie zonder toestemming ontbreekt.
Toestemming waarbij de betrokkene zich ervan bewust is waarvoor toestemming gegeven wordt, en weet dat hij/zij het recht heeft om dit verzoek te weigeren! Onder deze noemer valt ook het verstrekken van persoonsgegevens in een extern overleg.

Verstrekken van persoonsgegevens zonder toestemming

In bijzondere gevallen kan besloten worden om *zonder voorafgaande toestemming* persoonsgegevens te verstrekken aan derden. In het geval dat er sprake is van een zeer ernstige situatie of dringende noodzaak, of als vitale belangen van de betrokkene (of anderen) in gevaar zijn (bijvoorbeeld bij dringende zorg of huiselijk geweld). Of als er sprake is van noodzaak, maar pogingen om toestemming te krijgen niet geslaagd zijn of toestemming vragen niet mogelijk is.

Bij een dergelijke beslissing wordt altijd vooraf overleg gevoerd met minimaal één collega en de leidinggevende, en deze beslissing wordt met argumentatie vastgelegd in het dossier. De betrokkene wordt zo spoedig mogelijk geïnformeerd over de verstrekking, dit wordt alleen uitgesteld als er concrete aanwijzingen zijn dat de veiligheid van de betrokkene, gezin of anderen wordt bedreigd.

Recht op informatie, inzage, afschrift, correctie en vernietiging

Iedere inwoner, die tenminste 16 jaar oud is en '*in staat is tot een redelijke waardering van zijn belangen ter zake*'[12], heeft het *recht op inzage* in en eventueel een *afschrift (kopie)* van de *eigen* gegevens. Andere mensen mogen deze gegevens niet inzien. Er zijn twee uitzonderingen op deze regel:
a. de wettelijk vertegenwoordiger van de betreffende inwoner
b. of een jongere van minimaal 12 jaar als het een jeugddossier betreft. Deze jongere moet dan wel in staat zijn tot waardering van zijn belangen.

Elke inwoner heeft ook het *recht op correctie of vernietiging* als de vastgelegde gegevens onjuist zijn, of als er onvoldoende relatie is tussen de gegevens en het doel van verstrekken.

Een dossier kan gegevens van meerdere personen omvatten. En dat betekent dat we bij het behandelen van de vraag om inzage beoordelen of er *geen belangen van anderen geschaad kunnen worden*. Dat kan betekenen dat (delen van) het dossier niet ingezien mogen worden. Het is aan de medewerker om een zorgvuldige afweging te maken tussen het recht op inzage van de eigen gegevens en de belangen van de andere betrokkenen. Persoonlijke werkaantekeningen en stukken die nog in bewerking zijn, worden niet gezien als onderdeel van het dossier en worden niet ter inzage/als afschrift gegeven.

Inzage en afschrift kan worden gevraagd bij de medewerker die het dossier behandeld, of door een schriftelijke aanvraag in te dienen. Een verzoek voor correctie of vernietiging moet schriftelijk worden ingediend. Inzage, afschrift, correctie of vernietiging moet 'zo spoedig mogelijk' worden gerealiseerd. Als uitgangspunt hanteren wij afhandeling van de aanvraag binnen 4 weken (en daadwerkelijke vernietiging als dit wordt toegewezen binnen 3 maanden). Inzage in het dossier is gratis, voor een afschrift kunnen kosten in rekening worden gebracht. Deze kosten worden vooraf bekend gemaakt.

De wettelijk vertegenwoordiger

De wettelijk vertegenwoordiger oefent de rechten van een betrokkene uit:
1. als deze nog geen 12 jaar oud is;
2. samen met de betrokkene als deze 12 jaar of ouder is maar nog geen 16 jaar oud is;
3. als de betrokkene 16 jaar of ouder is, maar door de leidinggevende niet in staat wordt geacht tot '*een redelijke waardering van zijn belangen ter zake*'

Is er bij punt 3 geen wettelijk vertegenwoordiger, dan worden de rechten uitgeoefend door echtgenoot/ partner, ouder, meerderjarige broer of zus of meerderjarig kind. De leidinggevende kan de rechten beperken of weigeren op grond van zwaarwegende belangen van de betrokkene.

Bewaren en vernietigen van persoonsgegevens

We hebben de wettelijke plicht om informatie gedurende een bepaalde tijd te bewaren, en moeten deze daarna vernietigen. Wij bewaren en vernietigen persoonsgegevens op basis van vaste (en over het algemeen wettelijk/landelijk vastgestelde) bewaar- en vernietigingstermijnen die kunnen verschillen per soort 'zaak'.

Bezwaar- en klachtenprocedure

Als een betrokkene *bezwaar* heeft tegen verwerking van zijn/haar gegevens of als inzage, correctie of vernietiging wordt geweigerd dan kan hij/zij bezwaar indienen via de onafhankelijke gemeentelijke bezwaarprocedure.

Bezwaar kan worden gemaakt als er sprake is van een besluit in de zin van de algemene wet bestuursrecht. Belanghebbenden kunnen op grond van de regels van die wet bezwaar maken tegen besluiten van het college of die namens het college worden genomen in mandaat op verzoeken van betrokkene (of diens wettelijk vertegenwoordiger).

De volgende besluiten zijn aangewezen:
- Het besluit op een verzoek om inlichtingen over de van aanmelding vrijgestelde gegevensverwerkingen;
- Het besluit op een verzoek om inzage in de gegevens;
- Het besluit op een verzoek om correctie van de gegevens;
- Het besluit op een verzoek om opgave van de derden die u hebt ingelicht over een correctie;
- Het besluit op een verzet aangetekend op grond van artikel 40 of artikel 41 van de Wbp.

[12] Privacy reglement Bureau Jeugdzorg, artikel 13 lid 2

Het bezwaarschrift moet worden gericht:
Aan : Burgemeester en wethouders van Bussum
Adres : Postbus 6000, 1400 HA Bussum
Termijn : Binnen zes weken na bekendmaking van de beschikking
Kosten : Geen

Inwoners van Naarden en Muiden moeten hun bezwaarschrift tegen de verwerking van de persoonsgegevens bij het college van hun woonplaats indienen.

Inhoud van het bezwaarschrift

Een bezwaarschrift moet:
1. Ondertekend zijn;
2. De naam en het adres van de indiener bevatten;
3. Dagtekening bevatten (datum);
4. Omschrijving van het besluit waartegen het bezwaar is gericht bevatten;
5. De gronden van het bezwaar bevatten (waarom bent u het er niet mee eens).

Tenslotte kunnen inwoners bij het college van hun woonplaats een klacht (in het kader van de privacy) indienen. Hoe dat in zijn werk gaat, staat op de website van de betreffende gemeente.

Lijst van toepassing zijnde regelgeving

- Artikel 8 Europees Verdrag voor de Rechten van de Mens
- Artikel 10 Grondwet
- Artikel 272 Wetboek van strafrecht
- Wet bescherming persoonsgegevens (Wbp)
- Wet maatschappelijke ondersteuning (WMO)
- Wet op de jeugdzorg (Wjz), en vanaf 2015 de Jeugdwet
- Wet en besluit politiegegevens
- Wet inzake de geneeskundige behandelingsovereenkomst
- Wet op de beroepen in de individuele gezondheidszorg
- Archiefwet, archiefbesluit en archiefregelingen
- Beroepscode van de Nederlandse Vereniging van Maatschappelijk Werkers
- Gedragscode van het Nederlands Instituut voor Psychologen
- Gedragscode van de Nederlandse Vereniging voor Onderwijskundigen en Pedagogen
- Handreiking Bemoeizorg van KNMG, GGD Nederland en GGZ Nederland

Tien Gouden regels

De 10 gouden regels voor het gebruik van informatie, informatiesystemen en netwerken, zoals bij de medewerkers van Sociale Zaken wordt uitgedragen.

Wij vragen even om jouw aandacht!
Afhankelijk van jouw functie heb jij toegang tot diverse informatiesystemen binnen SoZa. Wij willen je erop attenderen dat het gebruik van deze systemen verbonden is aan een aantal verplichtingen. Met deze tien gouden regels vatten wij de belangrijkste hiervan samen. Wij verzoeken je deze goed door te lezen omdat zij deel uitmaken van je functie binnen SoZa.

1. Wachtwoorden zijn strikt persoonlijk
Je wachtwoorden zijn strikt persoonlijk en dienen uitsluitend door jou gebruikt te worden om toegang te krijgen tot de betreffende systemen. Geef je wachtwoord dus niet aan derden of een collega en bewaar ze op een veilige plek, dus niet in je agenda of op een geel briefje!

2. Melden van beveiligingsincidenten
Binnen de gemeente waar je werkt is een collega belast met het uitvoeren van activiteiten rond het thema informatiebeveiliging. Bij ons is dat de Applicatie beheerder SoZa. Het is belangrijk om dit te weten, omdat beveiligingsincidenten bij deze persoon zo snel als mogelijk gemeld dienen te worden. Voorbeelden voor incidenten zijn een virusmelding op het systeem, waarmee je op dat moment werkt, een inbraak of een poging tot inbraak, of een deur die op slot had moeten zijn maar niet op slot is.

3. Geheimhoudingsplicht
Binnen SoZa wordt veel met persoonsgegevens gewerkt. Voor het werken en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (WBP). In de wet SUWI en in de CAO zijn daarom geheimhoudingsbepalingen opgenomen die inhouden dat je de persoonsgegevens niet verder bekend mag maken dan voor de uitoefening van je functie noodzakelijk is. Dit betreft persoonsgegevens die jou uit hoofde van je functie bekend worden, alsmede overige informatie waarvan je weet of redelijkerwijze kunt vermoeden dat geheimhouding verplicht is.

4. Gedragscode Internet- en e-mail-gebruik
In de gedragscode Internet- en e-mailgebruik zijn regels neergelegd die aangeven hoe de medewerkers behoren om te gaan met Internet en e-mail op de werkplek. Tevens bevat de code regels voor de manier waarop controle op het gebruik van de werkplek kan plaatsvinden. Deze gedragscode is op het Intranet te vinden.
E-mail verkeert geldt inmiddels als algemeen geaccepteerde correspondentie, gelijk aan brieven. E-mails kunnen, mits de betrouwbaarheid van het e-mail adres voldoende is aangetoond, gelden als bewijsstuk. Een e-mail is als het ware schriftelijke correspondentie, al dan niet voorzien van een handtekening, dat door middel van een elektronisch medium wordt verstuurd. (denk hierbij ook aan wettelijke eisen op het gebied van archivering)
Bovenstaande alinea is enkel van toepassing voor e-mail verkeer tussen onze dienst en instanties !
Kontaktpersonen kunnen door middel van het verzenden van e-mails op een snelle manier informatie uitwisselen over individuele klanten.
E-mail verkeer tussen klanten en medewerkers wordt ten zeerste afgeraden omdat deze correspondentie niet centraal wordt geregistreerd (voorzetting huidige werkwijze).
E-mails die klanten versturen aan hun kontaktpersoon worden niet gezien als bewijsstuk.

5. Kennisnemen van het informatiebeveiligingsbeleid
Het binnen de afdeling SoZa geldende informatiebeveiligingsbeleid en de bijbehorende richtlijnen, instructies en protocollen zijn op iedereen van toepassing. Vraag je leidinggevende voor meer informatie hierover.

6. Gegevensverstrekking aan derden via de telefoon
Het uitgangspunt is dat er niet aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen. Dat betekent dat er ook geen telefonische informatie over klanten wordt verstrekt aan personen of instanties die beweren namens de betrokkene te bellen. Vragen dienen schriftelijk te worden ingediend. Enkel in uitzonderlijke gevallen kan informatie verstrekt worden aan derden, indien de identiteit van deze voldoende vastgesteld kan worden (bijvoorbeeld door middel van terugbellen via een centraal telefoonnummer) en een schriftelijk verzoek tot informatie niet mogelijk is.

7. Clear desk / clear screen policy
De vertrouwelijke omgang met persoonsgegevens houdt o.a. in dat elke werkplek zodanig is ingericht, dat onbevoegden niet in jou afwezigheid aan deze gegevens kunnen komen. Dat betekent dat jij je werkstation

bewust dient te vergrendelen met behulp van de screensaver wanneer jij je werkplek verlaat. (kan zeer snel door het gelijktijdig indrukken van de Windows-toets + L)
Ook mogen geen vertrouwelijke gegevens, zoals dossiers of verslagen, onbeheerd op je bureau of in een niet afsluitbare kast blijven liggen.

8. Geen vertrouwelijke gegevens in de prullenbak
De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen de afdeling Sociale Zaken. Ook het vernietigen van deze gegevens moet op een veilige manier plaats vinden. Daarom zijn er special gekenmerkte papiercontainers aanwezig. Maak hiervan gebruik en stop vertrouwelijke gegevens nooit in de prullenbak of in een bak op je kamer die bestemd is voor oud-papier.

9. Aanspreken van onbekende personen zonder bezoekersbadge
Ben je al een keer in de situatie geweest, dat je iemand binnen het gebouw tegenkwam, waar officieel geen publiek zonder begeleiding mag komen en je niet wist wie deze persoon was en wat zij daar te doen had? Spreek deze persoon aan, stel jezelf voor en vraag, wat hij of zij hier komt doen. Nieuwe collega's, uitzendkrachten of ander ingehuurd personeel stellen het op prijs om aangesproken te worden en op deze manier contacten te kunnen leggen. Echter, personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Wijs hun beleeft, maar duidelijk, de weg naar het publieke gedeelte van het gebouw en – belangrijk – begeleidt ze daar naartoe.

10. Haast, stress, werkdrukte vs. informatiebeveiliging
Informatiebeveiliging krijg je niet gratis – het kost je energie en werkt vaak tegen je als je haast hebt en de werkdrukte hoog is. Echter, informatiebeveiliging is uitermate belangrijk voor je werk en hoort bij de professionele en bekwame uitvoering van het werk. Neem het daarom zeer serieus – je cliënten vertrouwen erop!