gemeente Staphorst

GEMEENTEBLAD

Officiële uitgave van de gemeente Staphorst

Nr. 409931

25 september 2023

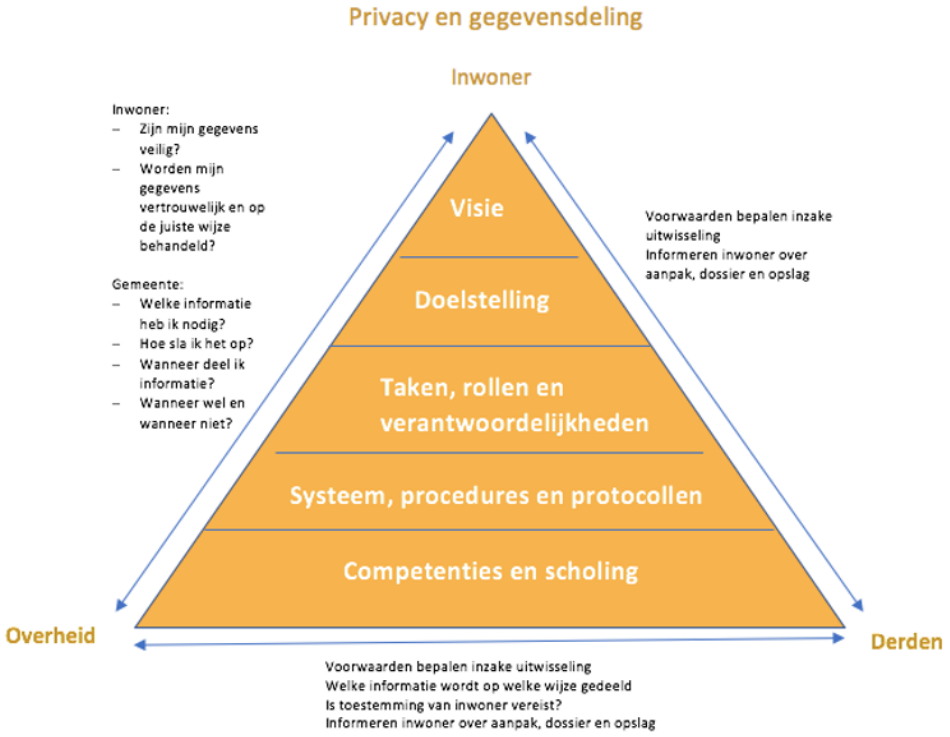
Privacybeleid gemeente Staphorst

Inleiding

Gemeenten hebben een belangrijke taak in de bescherming van de persoonsgegevens van hun inwoners. Persoonsgegevens en de uitwisseling daarvan vindt nagenoeg op elke afdeling plaats; tussen de verschillende afdelingen en met externe samenwerkingspartners. Met de wettelijke taken binnen het sociaal domein zijn de privacygevoelige gegevens binnen de gemeentelijke organisatie toegenomen. Inwoners hebben een groot belang bij een zorgvuldige omgang met deze gegevens. Zij hebben het recht om geïnformeerd te worden op welke wijze de gemeente de privacy borgt. Daarbij is ook het belang voor de gemeente groot.
Met de aangescherpte regelgeving naar aanleiding van de Algemene Verordening Gemeenten (AVG) heeft de gemeente de verantwoordelijkheid om de rechten van inwoners op het gebied van privacy goed te regelen. Als de gemeente dit niet goed regelt, loopt de gemeente risico's (o.a. imagoschade en financiële schade) als er niet (aantoonbaar) op een correcte wijze wordt omgegaan met persoonsgegevens. Er zijn bijna dagelijks berichten in het nieuws over datalekken. Privacybeleid en informatiebeveiligingsbeleid zijn hiermee urgente onderwerpen.

Binnen de bestaande wetgeving lijkt een dilemma te bestaan, enerzijds wordt aan gemeenten opgedragen om zoveel mogelijk integraal te werken (breed inventariseren en integraal handelen) en anderzijds wordt binnen de privacywetgeving doelbinding benadrukt. Doelbinding betekent dat alleen die informatie mag worden opgevraagd en verwerkt die nodig is voor het doel waarvoor het wordt aangevraagd. Bijvoorbeeld als een inwoner een uitkering aanvraagt en met dit doel informatie verstrekt aan de gemeente, dan mag deze informatie niet zonder meer ook gebruikt worden voor de aanvraag van een andere voorziening.

Het is mogelijk om deze twee uitersten te verbinden, dus zowel de wetgeving te volgen als ook een werkbaar geheel te creëren. Dit vraagt echter wel om een eenduidige formulering van de visie op privacy en gegevensdeling binnen de gemeentelijke organisatie en een eenduidige inrichting van de werkprocessen, maximaal ondersteund middels een helder kader en ICT-ondersteunende processen. Als laatste dient er ook te worden geïnvesteerd in de benodigde competenties van alle betrokkenen en in het vergroten van de bewustwording. Zie ook onderstaande afbeelding.



gemeente Staphorst

Hoofdstuk 1. Privacybeleid

Dit privacybeleid is opgesteld om te bepalen hoe de gemeente Staphorst om wil gaan met persoonsgegevens van haar inwoners en ondernemers, maar ook van personen uit andere gemeenten en andere landen. In dit beleid is weergegeven wat de visie en ambities van de gemeente Staphorst op dit terrein zijn. Daarnaast is in dit beleid de Europese en landelijke regelgeving verwerkt en wordt weergegeven welke consequenties die regelgeving heeft voor de organisatie van de gemeente Staphorst.

In dit document zijn de eisen van de Algemene Verordening Gegevensbescherming (vanaf nu: AVG) vertaald naar concrete, hanteerbare normen die duidelijk aangeven *waar* de gemeente Staphorst *wat* moeten regelen in zijn privacybeleid, in de uitvoering en in de controle op dit beleid.

1.1 Waarom Privacybeleid

Voldoen aan de wettelijke voorschriften is één doel, maar niet het enige. Door dit privacybeleid te hanteren wil de gemeente Staphorst op een goede, verantwoorde en veilige manier omgaan met alle persoonsgegevens die de gemeente verwerkt of verzamelt. De gemeente Staphorst wil een betrouwbare partner zijn.

Op basis van dit beleid en op basis van een privacyscan, die eind 2017 is uitgevoerd, is een plan van aanpak opgesteld, waarin is beschreven wat de gemeente Staphorst nog moet regelen om te voldoen aan de wetgeving en haar visie en ambities rond privacy in de praktijk vorm te geven.

Voor wie is dit privacybeleid van toepassing?
Om in één oogopslag te kunnen zien of er sprake is van gegevensverwerking in de zin van de AVG en of deze verwerking van persoonsgegevens op basis van de AVG is toegestaan, is onderstaand schema opgesteld. Dit schema is bedoeld als quick scan om te beoordelen of het privacybeleid van toepassing is.

	Vraag	Antwoord
Vraag 1	Wil/moet ik persoonsgegevens (zie 2.2.1 Persoonsgegeven) verwerken?	Nee? De AVG (en dus dit Privacybeleid) is niet van toepassing.
Vraag 2	Kan ik deze verwerking baseren op een van de rechtmatige gronden van de AVG (zie 2.2.2 Verwerking Persoonsgegevens en 2.2.3 Rechtmatige gronden voor de verwerking van persoonsgegevens)?	Is het antwoord op vraag 1 'ja', maar is het antwoord op vraag 2 'nee'? U mag geen persoonsgegevens verwerken.

1.2 Wettelijk kader

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de gehele Europese Unie (EU). De Algemene Verordening Gegevensbescherming (AVG) vervangt de Wet bescherming persoonsgegevens (Wbp). De gemeente heeft dus tot eind mei 2018 om de AVG te implementeren.

Wanneer de gemeente persoonsgegevens wil of moet verwerken, dient zij hiervoor een rechtmatige grond te hebben en te voldoen aan de AVG en de sectorspecifieke wetgeving (Wmo, Jeugdwet, Participatiewet, Omgevingswet etc.).

De AVG herbergt veel uitgangspunten die ook in de Wbp waren opgenomen, maar bevat daarnaast een aantal nieuwe elementen. Zo worden de privacyrechten van mensen versterkt en uitgebreid, krijgen organisaties meer verantwoordelijkheden en kunnen er door de autoriteiten stevige boetes worden opgelegd. In de volgende paragraaf gaan we hier nader op in.

1.3 Wat er verandert

De AVG bevat een aantal nieuwe elementen ten opzichte van de oude wetgeving (Wet bescherming persoonsgegevens).

Wat er verandert voor inwoners
De AVG geeft mensen meer mogelijkheden om voor zichzelf op te komen bij de verwerking van hun gegevens. Hun privacyrechten worden namelijk versterkt en uitgebreid. In de AVG staat bijvoorbeeld een speciaal artikel over toestemming. Hierin staat wat de voorwaarden zijn voor organisaties om geldige toestemming te krijgen van mensen om hun persoonsgegevens te verwerken.

Zo moeten organisaties kunnen bewijzen dat zij geldige toestemming hebben gekregen. Daarnaast moet het voor mensen net zo makkelijk zijn om hun toestemming in te trekken als om die te geven.

Hierbij moet worden opgemerkt, dat de gemeente niet alleen maar gegevens verwerkt van haar eigen inwoners en ondernemers, maar ook van personen uit andere gemeenten en andere landen. Denk hierbij aan het noteren van kentekens van auto's in de gemeente Staphorst, verwerking van gegevens van jeugdigen uit een andere gemeente in het kader van de Jeugdwet en dergelijke.

Naast versterking van de bestaande rechten krijgen mensen door de AVG een aantal aanvullende rechten, zoals bijvoorbeeld het recht op vergetelheid, het recht op inzage en het recht op dataportibiliteit. Een uitgebreide beschrijving van alle rechten die mensen op basis van de AVG krijgen is terug te vinden in paragraaf 4.1.2.

Wat er verandert voor de gemeente Staphorst
Door de AVG heeft de gemeente meer verplichtingen bij het verwerken van persoonsgegevens. De AVG legt namelijk meer nadruk gelegd op de verantwoordelijkheid van de gemeente om aan te tonen dat deze zich aan de wet houdt. Dit heet de verantwoordingsplicht.

De verantwoordingsplicht houdt in dat de gemeente Staphorst met documenten kan aantonen dat zij de juiste organisatorische en technische maatregelen heeft genomen om aan de AVG te voldoen, waarbij de nodige waarborgen moeten worden ingebouwd (art. 25 AVG). Maar de AVG biedt tegelijkertijd meer instrumenten die helpen om de wet na te leven, zoals modelbepalingen voor het doorgeven van persoonsgegevens.

Verder moet de gemeente een register bijhouden van verwerkingsactiviteiten (art. 30 AVG) en moet de gemeente Staphorst een functionaris voor de gegevensbescherming (FG) aangesteld hebben (art. 37 AVG). Deze functionaris heeft een onafhankelijke positie binnen de organisatie. De FG moet tijdig worden betrokken bij alles wat verband houdt met de bescherming van persoonsgegevens. Meer over het register van verwerkingsactiviteiten en over de functie en rol van de FG wordt weergegeven in paragraaf 2.1.

1.4 Privacybescherming
Het uitgangspunt van privacybescherming is dat iedereen de mogelijkheid moet hebben om na te gaan waar zijn persoonsgegevens worden vastgelegd en verwerkt, waarom en door wie. De bescherming van de privacy kan worden uitgedrukt in de zogeheten ACT-doelen: Afscherming, Corrigeerbaarheid en Transparantie.

Deze doelen kunnen als volgt worden beschreven:
Afscherming: Afscherming zorgt ervoor dat persoonsgegevens niet op een onrechtmatige manier kunnen worden verwerkt, zoals het gebruiken, doorgeven of koppelen van persoonsgegevens voor andere doelen dan de oorspronkelijke of voor onbekende doeleinden.

Corrigeerbaarheid: Tijdens en na elke verwerking van persoonsgegevens is het mogelijk om de persoonsgegevens en de uitkomsten van de verwerking aan te passen, indien deze niet voldoen aan de doelbinding of de kwaliteitsvereisten en daardoor de betrokkene (kunnen) benadelen.

Transparantie: Voor, tijdens en na de elke verwerking van persoonsgegevens is duidelijkheid over de doelbinding, de wettelijke grondslag en de organisatorische en technische inrichting van verwerking van de persoonsgegevens.

Hoofdstuk 2 Wetgeving

Zoals gezegd wordt de aanleiding voor dit privacybeleid gevormd door de inwerkingtreding van de AVG in 2018. In dit hoofdstuk wordt weergegeven welke gevolgen die wetgeving heeft voor de gemeente Staphorst, welke begrippen er in de wetgeving gebruikt worden en wat de relatie van dit privacybeleid met het informatieveiligheidsbeleid is.

2.1 Wat betekent de AVG voor de gemeente Staphorst?
De AVG vraagt van de gemeente Staphorst dat zij een aantal zaken geregeld heeft:

- De AVG verplicht de gemeente om een functionaris gegevensbescherming (FG) aan te stellen (art. 37 AVG). Deze functionaris heeft een onafhankelijke positie binnen de organisatie.
  De FG moet tijdig worden betrokken bij alles wat verband houdt met de bescherming van persoonsgegevens en heeft een cruciale rol in de borging van de zorgvuldige omgang met persoonsgegevens. De FG:
  - informeert en adviseert de gemeente inzake de bescherming van persoonsgegevens;
  - ziet toe op de naleving van de AVG;

- werkt samen met de Autoriteit Persoonsgegevens;
- kan benaderd worden door inwoners inzake de beveiliging van persoonsgegevens.

- Datalekken moeten 'onverwijld' worden gemeld bij de Autoriteit Persoonsgegevens (art. 33 AVG). 'Onverwijld' betekent volgens de richtsnoeren van de AP twee werkdagen. De uiterste tijdslimiet uit de AVG spreekt echter van melding binnen 72 uur. Houdt het datalek een hoog risico in voor de rechten en vrijheden van de inwoner, dan moet de gemeente de inwoner onmiddellijk informeren, behalve wanneer passende beveiligingsmaatregelen (zoals versleuteling) zijn genomen. Voor meer over deze meldplicht, zie paragraaf 2.3.
  Het melden van een datalek was ook onderdeel van de Wet Bescherming Persoonsgegevens, maar is in de AVG verder aangescherpt.
- Ter bescherming van persoonsgegevens moet de gemeente passende technische en organisatorische maatregelen nemen om de gegevensverwerking op een doeltreffende manier uit te voeren, waarbij de nodige waarborgen moeten worden ingebouwd (art. 25 AVG).
  Alleen persoonsgegevens die noodzakelijk zijn voor een specifiek doel mogen worden verwerkt. Wanneer de gemeente opdrachtgever is voor derden die persoonsgegevens verwerken, dan moeten er voldoende garanties zijn dat de rechten van de inwoner worden beschermd (art. 28 AVG). Eén van de manieren om dit te doen is het afsluiten van verwerkersovereenkomsten.
- De gemeente moet een register bijhouden van verwerkingsactiviteiten (art. 30 AVG) met daarin:
  - naam en contactgegevens van de verwerkingsverantwoordelijke(n);
  - de verwerkingsdoeleinden;
  - een beschrijving van categorieën van personen en van persoonsgegevens;
  - de categorie van ontvangers aan wie persoonsgegevens worden verstrekt;
  - de termijn waarbinnen persoonsgegevens moeten worden gewist;
  - een algemene omschrijving van de technische en organisatorische beveiligingsmaatregelen.

- De gemeente neemt passende technische en organisatorische maatregelen om het gewenste beveiligingsniveau te waarborgen (art. 32 AVG);
  - door pseudonimisering en versleuteling van persoonsgegevens;
  - door de vertrouwelijkheid, integriteit, en beschikbaarheid van verwerkingssystemen en diensten te garanderen;
  - door fysieke of technische incidenten te herstellen;
  - door de beveiligingsprocedures te testen, beoordelen en evalueren.

- Het is zaak om in de systemen waarin persoonsgegevens worden verwerkt zekerheden in te bouwen waarmee oneigenlijk gebruik zoveel mogelijk wordt voorkomen. Tegelijkertijd moet de medewerker liefst alle gegevens hebben die noodzakelijk zijn om de inwoner goed van dienst te zijn. Daarbij heeft de gemeente Staphorst gekozen voor een integrale werkwijze. Bij die werkwijze zijn het hergebruik en/of koppelen van gegevens soms van belang om zoveel mogelijk integraal te kunnen werken. Denk hierbij aan het adagium '1 gezin, 1 plan, 1 regisseur'. Op basis van dat adagium wil de gemeente Staphorst soms breed uitvragen tijdens een keukentafelgesprek of bepaalde gegevens aan elkaar kunnen koppelen. Dit kan op gespannen voet staan met de AVG en daarom dient dit op een veilige wijze plaats te vinden. Meer hierover is te lezen in bijlage 1: de AVG en de Zelfredzaamheidsmatrix.
- De AVG verplicht gemeenten om logsystemen in te richten, waarin de loggegevens worden geregistreerd. Deze loggegevens geven inzicht in de omgang met persoonsgegevens en kunnen aanleiding geven om op het niveau van de individuele medewerker onderzoek te doen. Binnen de praktijk van SUWI-net is dit al jaren geregeld.
- Het is zaak om de medewerkers van de gemeente Staphorst goed te trainen en daarnaast technische maatregelen te nemen voor de bescherming van persoonsgegevens.
- De inwoner moet geïnformeerd worden over het verzamelen van zijn persoonsgegevens bij derden, denk bijvoorbeeld aan SUWI-net, BAG, gemeentelijke belastingen, vergunningen. Het is raadzaam om dit standaard te doen op het moment dat een uitkering, vergunning of een ontheffing wordt aangevraagd.
- Verder heeft de gemeente de verplichting om inwoners actief te informeren wanneer bij derden persoonsgegevens worden opgevraagd. Dit kan voorkomen in het geval van een verhuizing, de aanvraag van een uitkering of bij een handeling in het kader van de wet Bibob. Worden die gegevens later gebruikt voor een ander doel, dan moet de inwoner weer worden geïnformeerd. Dit is een aandachtspunt: medewerkers zijn niet gewend dit te doen en deze verplichting kan administratief een belasting worden. In sommige gevallen hoeft de gemeente inwoners niet actief te informeren, namelijk wanneer in de betreffende materiewet is vastgelegd dat deze informatie nodig is voor de uitvoering van die materiewet. Dit komt bijvoorbeeld voor in het kader van de Jeugdwet.

Risico's

Het niet-voldoen aan de AVG leidt tot schending van de informationele privacy van degene op wie de gegevens betrekking hebben. Dit kan verregaande (negatieve) consequenties hebben: niet alleen voor de persoon in kwestie, maar ook voor de gemeente Staphorst. Zo kan het niet-voldoen aan de AVG (of zelfs de schijn daarvan) leiden tot negatieve publiciteit en imagoschade voor de organisatie.

En niet te vergeten: het niet-voldoen aan de AVG kan leiden tot juridische consequenties, waaronder:
- een door de rechter opgelegd verbod op het handelen van de organisatie en de verplichting tot het treffen van herstelmaatregelen bij (dreiging van) schade;
- vergoeding van de schade die de betrokkene heeft geleden;
- een bestuurlijke boete, opgelegd door de AP;
- een last onder bestuursdwang of dwangsom door de AP:
  - een last onder bestuursdwang houdt in dat de AP kan eisen de overtreding te beëindigen en bij het uitblijven daarvan dit 'persoonlijk' kan komen doen;
  - een last onder dwangsom houdt in dat de organisatie nog tijd heeft om de overtreding (gedeeltelijk) te herstellen en de dwangsom wordt opgelegd bij het uitblijven van het (gedeeltelijk) herstel.

- strafrechtelijke vervolging door het Openbaar Ministerie.

Voorts brengt elke eis die de AVG stelt een eigen risico met zich mee, wanneer er niet aan voldaan wordt.

2.2 Begrippen van de AVG in het Privacybeleid
De AVG hanteert een aantal begrippen, waarvan er veel ook in dit document worden gehanteerd. Omwille van eenduidigheid worden enkele begrippen toegelicht.

- persoonsgegevens;
- verwerking van persoonsgegevens;
- rechtmatige gegevensverwerking;
- rechtmatige gronden voor de verwerking van persoonsgegevens;
- betrokkene;
- verantwoordelijke;
- verwerker;
- Autoriteit Persoonsgegevens;
- nodige maatregelen/waarborgen.

2.2.1 Persoonsgegevens
Persoonsgegeven:
Elk gegeven betreffende een geïdentificeerde of identificeerbare, natuurlijke, levende persoon.

Persoonsgegevens kunnen direct of indirect identificeerbaar zijn.
- Direct identificeerbaar:
  gegevens die naar hun aard rechtstreeks betrekking hebben op een persoon, zoals iemands naam.
- Indirect identificeerbaar:
  gegevens die naar hun aard geen betrekking hebben op een persoon worden als persoonsgegeven aangemerkt als deze medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld. Voorbeelden hiervan zijn het type huis of auto van een betrokkene, omdat dit iets zegt over het inkomen en vermogen van de betrokkene. Ook gegevens die in combinatie met andere gegevens tot identificeerbaarheid kunnen leiden worden aangemerkt als persoonsgegeven.

Bijzondere persoonsgegevens
Dit zijn gegevens over:

- godsdienst of levensovertuiging;
- ras;
- politieke gezindheid;
- gezondheid;
- seksuele leven;
- lidmaatschap van een vakvereniging;
- strafrechtelijke persoonsgegevens;
- persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag;

- een wettelijk voorgeschreven identificatienummer (zoals een BS-Nummer of een kentekennummer).

Bijzondere persoonsgegevens zijn naar hun aard vertrouwelijker dan 'gewone' persoonsgegevens en verwerking ervan geschiedt op andere gronden dan 'gewone' persoonsgegevens.

2.2.2 De verwerking van persoonsgegevens

Verwerking: het begrip 'verwerking' is heel breed en omvat alle handelingen van verzameling tot vernietiging van persoonsgegevens. Ook 'simpele' handelingen zoals opslag of inzage van persoonsgegevens vallen onder het begrip verwerken.

Het is voor organisaties belangrijk om zich goed te realiseren dat doorgifte van persoonsgegevens naar personen en organisaties in landen binnen de EU (en dus binnen Nederland, ook bij personen of afdelingen binnen de eigen organisatie) ook onder het algemene begrip 'verwerking' valt. Op elke doorgifte van persoonsgegevens binnen de EU zijn dus alle wettelijke eisen die voor verwerking gelden van toepassing. De oorspronkelijke verantwoordelijke – dat is hij die het doel en de middelen voor de verwerking vaststelt – blijft dus ook na de doorgifte verantwoordelijk voor een rechtmatige omgang met persoonsgegevens en is dus ook (juridisch) aansprakelijk als er een onrechtmatigheid in de omgang met persoonsgegevens optreedt. De ontvangende partij is de verwerker van de persoonsgegevens. Tussen de verstrekker en ontvanger dient dus te allen tijde verplicht een verwerkersovereenkomst opgesteld te zijn.

Voor doorgifte van persoonsgegevens naar personen en organisaties in landen buiten de EU en de EER gelden andere/aanvullende gronden en eisen. De hoofdregel is dat een organisatie persoonsgegevens alleen mag doorgeven naar derde landen met een passend beschermingsniveau. Buiten die gevallen is doorgifte slechts toegestaan op basis van een wettelijke uitzondering of met een vergunning van de minister van Veiligheid en Justitie.

Hoewel niet limitatief, vallen de volgende handelingen in ieder geval onder verwerking van persoonsgegevens: verzamelen, vastleggen, bewaren, ordenen, wijzigen, opvragen, raadplegen, gebruiken, samenbrengen, met elkaar in verband brengen (koppelen), afschermen, uitwissen, vernietigen, profilen en doorgifte (elke vorm van ter beschikkingstelling, zoals doorzending en verspreiding). Kortom; alles wat je doet met persoonsgegevens, valt onder het begrip verwerken.

2.2.3 Rechtmatige gegevensverwerking

Een gegevensverwerking is rechtmatig als deze voldoet aan de eisen die de AVG, sectorspecifieke wetgeving en/of een (eventuele) Gedragscode stelt. De AVG eist dat persoonsgegevens:

a) op een behoorlijke en zorgvuldige manier, conform de wet worden verwerkt;
b) slechts worden verwerkt op basis van een van de limitatief in de AVG genoemde gronden;
c) slechts verder worden verwerkt voor doelen die verenigbaar zijn met de oorspronkelijke doelen of als er een rechtvaardigingsgrond voor de verdere verwerking is;
d) aan bepaalde kwaliteit voldoen;
e) adequaat beveiligd worden;
f) transparant worden verzameld, (verder) verwerkt en bewaard;
g) gegevens niet langer worden bewaard dan noodzakelijk is om het doel te bereiken.

2.2.4 Rechtmatige gronden voor de verwerking van persoonsgegevens

Persoonsgegevens mogen alleen worden verzameld en verwerkt op basis van een van de volgende limitatieve gronden:

- de betrokkene heeft zijn uitdrukkelijke toestemming gegeven voor de verwerking;
- de gegevens zijn door de betrokkene zelf duidelijk openbaar gemaakt of de verwerking is noodzakelijk;
- voor de juridische vaststelling, de uitoefening of de verdediging van een recht;
- ter verdediging van de vitale belangen van de betrokkene of van een derde en het vragen van diens uitdrukkelijke toestemming onmogelijk blijkt;
- ter voldoening aan een volkenrechtelijke verplichting;
- met het oog op een zwaarwegend algemeen belang, indien passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel de AP ontheffing heeft verleend. De AP kan bij de verlening van ontheffing beperkingen en voorschriften opleggen. Verwerkingen op deze grond worden bij de Europese Commissie gemeld. De Minister van V&J verricht de melding indien de verwerking op deze grond bij wet is voorzien. De AP verricht de melding indien de AP voor de verwerking op deze grond ontheffing heeft verleend;

- de gegevens worden verwerkt door de AP of een Ombudsman wanneer dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, voor de uitvoering van de hun wettelijk opgedragen taken en bij die uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Het voorgaande houdt in dat er een goed omschreven werkinstructie moet komen met daarin een toestemmingsformulier, dat goed bevonden is door de AP. Dit toestemmingsformulier is bijgevoegd in bijlage 2. Verder moeten er werkinstructies komen die omschrijven waarom bepaalde informatie gebruikt wordt en waarom deze informatie opgevraagd kan worden bij mensen.

De consequenties van deze punten zijn:
- Bij elke verwerking zal vastgelegd moeten zijn wat de grondslag van de verwerking is, wat verwerkt wordt en waarom dat noodzakelijk is. Dit zal gecommuniceerd moeten worden naar de burger. Deze punten moeten ook terugkomen in eenduidige werkinstructies naar de uitvoerder;
- Indien er geen grondslag ligt in de wet, moet met toestemming gewerkt worden, Het niet verlenen van toestemming mag niet leiden tot nadeel voor de betrokkene. Ook dit moet eenduidig naar de betrokkene worden gecommuniceerd en eenduidig in de werkinstructies worden vastgelegd;
- Er zal een zeer goede instructie en beleidsregel geschreven moeten worden wanneer en waarom een “Breaking the glass” procedure gevolgd wordt, wie daarin de verantwoordelijke en proceseigenaar is. “Breaking the glass” houdt in dat er opgeschaald wordt om te voorkomen dat er handelingen plaatsvinden die niet voldoen aan de wetgeving. Hierbij zal ook moeten worden vastgelegd, hoe de stappen in de procedure gevolgd en vastgelegd worden.

Bijzondere persoonsgegevens worden slechts verwerkt ten behoeve van wetenschappelijk onderzoek of statistiek indien:

a) het onderzoek een algemeen belang dient en
b) de verwerking voor het betreffende onderzoek of de betreffende statistiek noodzakelijk is en
c) het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost, en
d) bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Indien aan al deze voorwaarden is voldaan mogen de gegevens ten behoeve van wetenschappelijk onderzoek worden verwerkt. Deze voorwaarden zijn vergelijkbaar met de voorwaarden onder de richtlijn. De AVG wijkt hierin in feite niet af van de Wet Bescherming Persoonsgegevens.

Een wettelijk voorgeschreven identificatienummer, zoals een BS-Nummer of een kentekennummer, is ook een bijzonder persoonsgegeven en mag slechts worden verwerkt ter uitvoering of bereiking van de doelen van de wet die het betreffende nummer heeft ingesteld of ter bereiking van een specifieke Algemene maatregel van bestuur.

De consequenties hiervan is dat er alleen gewerkt mag worden met niet tot een persoon herleidbare gegevens, en dit houdt in dat er bijvoorbeeld voor wijkanalyses en dergelijke alleen gewerkt mag worden met de gegevens die door het CBS worden verstrekt, of die gepseudonimiseerd zijn.

2.2.5 Betrokkene
Een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

De betrokkene is degene op wie een persoonsgegeven betrekking heeft. De betrokkene is géén eigenaar van zijn/haar data: eigendom van data is in juridische zin erg lastig. De term eigendom geldt eigenlijk alleen voor fysieke zaken; software en data vallen daar niet onder. Data ‘is’ niets. Omdat daarmee de rechtspositie van de maker en de gebruiker van de data zeer moeilijk te bepalen is, is het goed om met een toestemmingsformulier te werken. Een voorbeeld hiervan vindt u in bijlage 2.

2.2.6 Verwerkingsverantwoordelijke
De verantwoordelijke is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De verantwoordelijke is verantwoordelijk voor de nakoming van de plichten van de AVG en moet zorgdragen dat verwerkers aan de eisen voldoen. Tussen de verantwoordelijke en verwerker moet een schriftelijke verwerkersovereenkomst zijn gesloten waarin de afspraken en AVG-verplichtingen zijn opgenomen.

2.2.7 Verwerker
Een verwerker is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

De verwerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. Tussen de verantwoordelijke en verwerker moet een schriftelijke verwerkersovereenkomst zijn gesloten waarin de afspraken en AVG-verplichtingen zijn opgenomen.

2.2.8 Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens (AP) is de Nederlandse onafhankelijke toezichthouder op de rechtmatigheid van de omgang met persoonsgegeven. Met ingang van 1 januari 2016 heeft de AP de rol van het College Bescherming Persoonsgegevens overgenomen.

2.2.9 Nodige maatregelen/waarborgen
Het begrip 'nodige' duidt op een proportionaliteit tussen enerzijds het belang van de bescherming van persoonsgegevens en anderzijds de kosten en inspanningen die zijn verbonden aan de bedoelde voorzieningen. De aard van de vereiste voorzieningen zal wijzigen met de ontwikkeling van de stand van de techniek. Wat op het ene moment nog als proportionele maatregel kan worden gezien, is dat op een volgend moment niet meer. Het begrip ‘nodige’ zal dus worden afgewogen tegen de stand van de techniek en is daardoor in zekere zin onafhankelijk van die technologie.

2.3 Meldplicht Datalekken
In de AVG worden organisaties verplicht om een datalek te melden bij de AP en die meldplicht op te nemen in de verwerkersovereenkomst. Met de komst van de Meldplicht datalekken wordt elke inbreuk die leidt tot (de aanzienlijke kans dat) ernstige nadelige gevolgen voor de bescherming van persoonsgegeven intreden, aangemerkt als een datalek die gemeld moet worden aan in ieder geval de AP en in sommige gevallen ook aan de betrokkene. Met andere woorden: elk beveiligingsincident waarbij persoonsgegevens misbruikt zouden kunnen (gaan) worden, of persoonsgegevens verloren zouden kunnen (zijn) gegaan, is een datalek dat 'onverwijld' gemeld moet worden. Hierbij kan gedacht worden aan bijvoorbeeld hacking of verlies van een usb-stick, laptop of een smartphone met werkmail.

Een datalek zoals hierboven bedoeld moet zoals gezegd onverwijld gemeld worden bij de AP en aan een aantal inhoudelijke voorwaarden voldoen. De AVG hanteert een uiterlijke meldingstermijn van 72 uur. Deze voorwaarden zijn zodanig dat het uitermate raadzaam is de organisatie tijdig op orde te brengen en goed in te richten op het ontdekken, beoordelen en vastleggen van inbreuken. Hoewel een inbreuk op de AVG te allen tijde een slechte zaak is, gaat het in deze context niet alleen om de inbreuk, maar ook om het niet melden daarvan. Als de gemeente nalatig is in het (correct) melden van een datalek, kan die nalatigheid ook worden bestraft.

Heeft een inbreuk waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkenen, dan moeten ook zij een gespecificeerde kennisgeving en een advies ontvangen. Dat advies moet gaan over wat de betrokkene zelf eventueel nog kan doen om schade te beperken. Het bijzondere is hier dat de verantwoordelijke dus zelf een inschatting moet maken van de kans op ongunstige gevolgen voor betrokkenen. Wanneer wordt besloten om de inbreuk niet te melden, moet de verantwoordelijke dit aan de AP kunnen verantwoorden.

Boetes
In de AVG is de boetebevoegdheid van de Autoriteit Persoonsgegevens (AP) uitgebreid. De AP kan ook bij schending van meer algemene verplichtingen van de AVG boetes opleggen; bijvoorbeeld als persoonsgegevens niet op een behoorlijke en zorgvuldige manier zijn verwerkt of langer worden bewaard dan noodzakelijk.

2.4 Verbinding met Informatieveiligheidsbeleid
De voorschriften uit het Information Security Management System (ISMS), waar ook de BIG (Baseline Informatiebeveiliging Gemeenten) deel van uitmaakt, zijn meegenomen in dit document.

Er ligt een duidelijke verbinding tussen privacybeleid en informatiebeveiligingsbeleid.

Informatiebeveiliging en privacy overlappen elkaar en worden in de praktijk vaak als één gezien. Dit zorgt nog wel eens voor verwarring. Zo denken sommigen gemeenten dat als je aan de BIG voldoet, je voor 90% voldoet aan de privacywetgeving. Dit is niet het geval. Informatiebeveiliging en privacy zijn namelijk echt twee verschillende aandachtsgebieden. Informatiebeveiliging kan op onderdelen zonder privacy, privacy kan niet zonder informatiebeveiliging.

Informatiebeveiliging is een manier om cyberrisico's te verminderen en informatieveiligheid te verhogen. Dit kan door het nemen van administratieve, technische en 'fysieke' maatregelen. In relatie tot privacy gaat het binnen informatiebeveiliging meer om de 'hoe-vraag'. Privacy daarentegen gaat over de bescherming van de persoonlijke levenssfeer. Binnen privacy gaat het meer om de 'wat-' en de 'waarom-vraag'. Informatiebeveiliging maakt dus deel uit van privacy, maar is niet hetzelfde!

Hoofdstuk 3. Visie gemeente Staphorst

In dit hoofdstuk zijn de visie en ambitie van de gemeente Staphorst ten aanzien van privacy geformuleerd. De basis voor die visie en ambitie ligt in een aantal uitgangspunten die zijn opgenomen in de AVG. Die uitgangspunten worden in dit hoofdstuk verder uitgewerkt.

3.1 Visie op privacy gemeente Staphorst

Investeren in bewustwording en het aanleren van een juiste toepassing van privacyregels is een belangrijk onderdeel van het implementatieproces. Een gemeenschappelijke visie op privacy en gegevensuitwisseling, die is vertaald naar een gemeenschappelijk normenkader helpt hierbij.
De visie van de gemeente Staphorst wordt hierbij als vertrekpunt genomen. De visie van de gemeente Staphorst luidt als volgt:

De samenleving ontwikkelt zich voortdurend. De gemeente Staphorst beweegt flexibel mee en maakt gebruik van de kracht van die samenleving: de gemeente ontwikkelt zich van een regisserende, bepalende overheid naar een loslatende, voorwaardenscheppende, inwonergerichte overheid.

De gemeente Staphorst wil in verbondenheid met inwoners, bedrijven en maatschappelijke organisaties verantwoordelijkheid nemen voor de woon-, werk- en leefomgeving.

De kernwaarden waar de gemeente Staphorst voor staat zijn:
- *Verantwoordelijkheid*
- *Daadkracht*
- *Vertrouwen*
- *Participatie*

De gemeente Staphorst is een gemeente die dichtbij haar inwoners staat. De lijnen zijn kort en de medewerkers zijn verbonden met de sterke cultuur van de gemeente. Inwoners zijn in de gemeente Staphorst in het algemeen bekend met naam en toenaam. Dit is een kracht van de gemeente Staphorst, maar kan tegelijkertijd ook een valkuil zijn. Immers, de aangescherpte privacyregels vragen steeds om een juiste afweging op het delen van gegevens van inwoners. De gewoonte van de korte lijnen binnen de gemeente, kan hiermee doorkruist worden. Naast het inrichten van een eenduidig privacybeleid, vraagt het aanleren van een kritische houding inzake dit onderwerp ook om een cultuurverandering.

Als we bovenstaande visie vertalen naar het thema "Privacy en gegevensuitwisseling" dan is voor de verdere uitwerking van beleid het volgende van belang.

De visie van de gemeente Staphorst op privacy en gegevensuitwisseling is:
- verantwoordelijkheid dragen voor een juiste toepassing van de wetgeving inzake privacy en gegevensuitwisseling;
- transparant zijn naar inwoners over persoonsgegevens en uitwisseling daarvan;
- vertrouwen uitstralen dat de gemeente op juiste wijze met gegevens van inwoners omgaat;
- daar waar dit kan inwoners laten meedenken en meedoen over de ontwikkeling van privacybeleid

Normenkader
Om deze visie op privacy en gegevensuitwisseling te kunnen communiceren over het omgaan met privacy en gegevensdeling binnen de gemeente is het onderstaande normenkader als uitgangspunt voor het handelen geformuleerd.

Gemeenschappelijk normenkader:

Wij verzamelen alleen die informatie die nodig is voor het doel, gaan daar op een bewuste manier mee om en geven daardoor mensen het vertrouwen dat wij de privacy van mensen respecteren.
Hiervoor:
- volgen wij de van toepassing zijnde wetgeving
- zijn wij transparant over gegevensdeling
- vragen wij expliciet om toestemming indien nodig

- communiceren wij in begrijpelijke taal

3.2 Uitgangspunten AVG
Zoals in paragraaf 1.2 is beschreven kent de AVG een aantal uitgangspunten.

- *toestemmingsvereiste*, tenzij …
- *doelbinding*: persoonsgegevens mogen alleen worden verzameld en verwerkt met een specifiek doel.
- *zorgvuldigheid en juistheid*: de gemeente moet zorgvuldig met de persoonsgegevens omgaan en
- zorgen voor de juistheid van die gegevens;
- *minimale gegevensverwerking*: er moeten niet meer gegevens worden verwerkt dan noodzakelijk.

3.2.1 Het toestemmingsvereiste
Het uitgangspunt van de AVG is dat persoonsgegevens mogen worden verwerkt wanneer de inwoner daarvoor toestemming geeft (art. 6 en 7 AVG). Die toestemming moet in vrijheid worden verleend en mag dus niet onder druk van een afhankelijkheidsrelatie gegeven worden (de inwoner geeft toestemming omdat hij verwacht anders niet in aanmerking voor ondersteuning te komen).

De verwerking van persoonsgegevens is echter ook toegestaan wanneer;
- er een overeenkomst met de inwoner is;
- de gemeente moet voldoen aan een wettelijke verplichting;
- de vitale belangen van de inwoner of een derde in het geding zijn;
- het algemeen belang of de uitoefening van openbaar gezag dat noodzakelijk maakt;
- gerechtvaardigde belangen van de gemeente, behalve wanneer de belangen, grondrechten of fundamentele vrijheden van de inwoner zwaarder wegen.

Het bovenstaande betekent dat de gemeente in de praktijk maar zelden afhankelijk is van de toestemming van de inwoner. In het gros van de gevallen wordt namelijk voldaan aan een van de hiervoor genoemde punten, waarbij verwerking van persoonsgegevens is toegestaan. Dit wil echter niet zeggen dat de gemeente zich veel kan veroorloven. Het is juist extra reden om zorgvuldig met de persoonsgegevens van inwoners om te gaan.

Wanneer er door de inwoner toestemming wordt verleend voor de verwerking van persoonsgegevens, dan moet de gemeente dat later kunnen aantonen. Het is raadzaam om altijd schriftelijk toestemming te vragen. De toestemming kan altijd worden ingetrokken. Een kind van 16 jaar of ouder kan zelfstandig toestemming verlenen. Wanneer de toestemming wordt ingetrokken, dan moeten de verstrekte persoonsgegevens worden vernietigd.

3.2.2 Doelbinding
Er mogen alleen gegevens worden verzameld met een specifiek doel. Dat betekent echter niet dat alleen gegevens mogen worden verzameld die slechts betrekking hebben op de ondersteuningsvraag. Voorbeeld: een medewerker gaat naar een moeder met een opvoedingsvraag en verzamelt gegevens. Tijdens het gesprek blijkt dat er ook financiële problemen zijn. Daar mag op worden doorgevraagd, omdat daarmee gegevens worden verzameld met betrekking tot een nieuw doel; het oplossen van financiële problemen.
Het is ook niet zo dat gegevens die voor een specifiek doel zijn verzameld niet voor een ander doel mogen worden gebruikt. Wanneer zich een nieuw doel aandient en er zijn gegevens bekend die daarbij van toepassing zijn, dan mogen die gegevens worden gebruikt. Dit moet echter wel in een wettelijke grondslag moeten zijn ondergebracht. Het gaat hier bijvoorbeeld om het hergebruik van NAW-gegevens, verstrekt in de wettelijke taak vanuit de BRP, waarbij is vastgelegd in zowel de participatiewet, als in de BRP dat die gegevens weer gebruikt mogen worden binnen de participatiewet, en niet weer opnieuw hoeven te worden uitgevraagd. (Wet Eenmalige Uitvraag).

3.2.3 Zorgvuldigheid en juistheid
Zorgvuldigheid hangt samen met doelbinding. In zowel de Europese als de Landelijke wetgeving is nadrukkelijk gekozen om de grondslag voor de verwerking van persoonsgegevens in de sectorspecifieke wetgeving te zoeken. Hier is een spanningsveld met het integraal werken dat wordt nagestreefd. Het is bijvoorbeeld niet toegestaan om van elke inwoner waar de gemeente contact mee heeft allerlei gegevens op te halen om zodoende meerdere leefgebieden in kaart te brengen. Dit is op dit moment echter wel de praktijk bij de zogeheten keukentafelgesprekken. De opgehaalde informatie over de verschillende leefgebieden wordt verwerkt in een zelfredzaamheidsmatrix. Er mogen echter alleen gegevens

worden verzameld met een specifiek doel en het opstellen van een zelfredzaamheidsmatrix is geen specifiek doel in de zin van de AVG (Rapport AP: "Gemeenten verzamelen teveel persoonsgegevens bij uitvoering Wmo en Jeugdwet").

Uit het zorgvuldigheidsbeginsel komt een aantal eerdergenoemde verplichtingen voort. Zo moet er een Functionaris Gegevensbescherming worden aangesteld, dient er sprake te zijn van privacy by design, wat onder meer inhoudt dat er niet méér gegevens worden verzameld dan strikt noodzakelijk, moet er een Data protection impact assessment uitgevoerd worden, moet er gegevensbeschermingsbeleid vastgesteld worden en moet er een register van alle verwerkingen bijgehouden worden.

3.2.4 Minimale gegevensverwerking

Het aantal gegevens dat verzameld wordt, moet beperkt worden tot wat noodzakelijk is voor de doeleinden. Dit uitgangspunt omvat de principes van proportionaliteit (in relatie tot het doel) en subsidiariteit (kan het met minder persoonsgegevens dan moet het met minder persoonsgegevens).

Hoofdstuk 4. Vertaling naar de organisatie

4.1 Het Control- of Beheerdomein

Om privacybeleid en informatieveiligheidsbeleid een juiste plaats te geven in de organisatie, moeten die beleidsterreinen gekoppeld worden aan de reguliere planning en control cyclus. Zowel de AVG als de BIG schrijven voor dat er een regelmatige terugkoppeling moet zijn naar directie en gemeentebestuur. Hierdoor worden zowel de directie als het gemeentebestuur zich bewust van de risico's die gepaard gaan met het verwerken van informatie en persoonsgegevens. Deze risico's zijn divers, maar denk hierbij aan een datalek, imagoschade en (forse) boetes.

Het privacybeleid leidt tot een aantal acties die de gemeente moet ondernemen om haar visie en ambitie te realiseren. Deze acties zijn opgenomen in een plan van aanpak, waarin de doelstellingen en het bijhorend budget zijn geformuleerd. De voortgang van het plan is een integraal onderdeel van de P&C cyclus, en de rapportage naar de raad.

4.1.1 Intern toezicht

Intern toezicht wordt geleverd door de FG en de CISO. Dezen worden hierin bijgestaan door de intern auditors van de gemeente. Zowel informatieveiligheid als privacy zijn een onderdeel van de ENSIA (Eenduidige Normatiek Single Information Audit), en als zodanig een onderdeel gaan uitmaken van de accountantscontroles. Het koppelen van bepaalde werkzaamheden en planning aan het werk van de concerncontroller ligt hierbij voor de hand.

4.1.2 Toegang gegevensverwerking voor betrokkene

De inwoner heeft op basis van de AVG bepaalde rechten. De gemeente moet faciliteren dat deze rechten kunnen worden uitgeoefend.

Recht op informatie (artikel 13 en 14 AVG)
Een betrokkene moet op de hoogte worden gesteld van het feit dat verwerking van zijn persoonsgegevens plaatsvindt of zal plaatsvinden en wat de doeleinden hiervan zijn. De AVG geeft aan welke informatie in ieder geval verstrekt moet worden, bijvoorbeeld informatie over de periode, de rechten van betrokkene, de bron van gegevens en de juridische grondslag voor de verwerking. Verandert het doel van de verwerking, dan moet ook daarover informatie worden verstrekt.

Recht van inzage (artikel 15 AVG)
Betrokkenen hebben het recht te weten of hun betreffende persoonsgegevens worden verwerkt door de verantwoordelijke. De AVG bevat een opsomming van de informatie waarvoor het recht van inzage geldt. De verwerkingsverantwoordelijke moet betrokkene een kopie verstrekken van de persoonsgegevens die worden verwerkt.

Recht op rectificatie (artikel 16 AVG)
Betrokkene heeft recht op rectificatie van hem betreffende onjuiste persoonsgegevens dan wel het recht een aanvullende verklaring te verstrekken wanneer de verwerking plaatsvindt op basis van onvolledige gegevens. De rectificatie moet meteen plaatsvinden. De verwerkingsverantwoordelijke is verplicht iedere ontvanger aan wie persoonsgegevens zijn verstrekt in kennis te stellen van elke rectificatie, tenzij dit onmogelijk is of onevenredig veel inspanning vraagt.

Recht op gegevenswissing /vergetelheid (artikel 17 AVG)
De verwerkingsverantwoordelijke is verplicht persoonsgegevens van de betrokkene zonder onredelijke vertraging te wissen, onder andere indien:

- persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- de betrokkene zijn toestemming intrekt en er geen andere rechtsgrond voor verwerking bestaat;
- betrokkene bezwaar maakt tegen de verwerking;
- de persoonsgegevens onrechtmatig verwerkt zijn.

Recht op beperking van de verwerking (artikel 18 AVG)
Het recht op beperking houdt in dat de persoonsgegevens (tijdelijk) niet verwerkt mogen worden en niet gewijzigd mogen worden. Het feit dat de verwerking van de persoonsgegevens beperkt is, moet door de verwerkingsverantwoordelijke duidelijk in het bestand zijn aangegeven zodat dit ook duidelijk is voor ontvangers van de persoonsgegevens. Wanneer de beperking weer wordt opgeheven, moet de betrokkene hiervan op de hoogte worden gebracht.

Recht op overdraagbaarheid/ dataportibiliteit (artikel 20 AVG)
Dit recht houdt in dat een betrokkene de gegevens van een verwerkingsverantwoordelijke moet kunnen verkrijgen in gestructureerde, gangbare en machineleesbare vorm en het recht heeft deze gegevens aan een andere verwerkingsverantwoordelijke over te dragen of rechtstreeks te laten overdragen, zonder daarbij te worden gehinderd tenzij dit afbreuk doet aan rechten en vrijheden van anderen. Een betrokkene heeft recht op overdraagbaarheid voor zover het gaat om door hem zelf verstrekte gegevens.

Recht van bezwaar (artikel 21 AVG)
Een betrokkene kan vanwege redenen die verband houden met zijn specifieke situatie gebruik maken van dit recht van bezwaar (dat niet vergelijkbaar is met bezwaar op grond van de Awb) tegen de verwerking van hem betreffende persoonsgegevens, als voldaan wordt aan de in de verordening genoemde eisen. Als een betrokkene bezwaar maakt, staakt de verwerkingsverantwoordelijke de verwerking, tenzij dwingende gerechtvaardigde gronden anders bepalen.

Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming/ profiling (artikel 22 AVG)
Bij dit recht kan bijvoorbeeld gedacht worden aan de automatische weigering van een online ingediende kredietaanvraag of aan de verwerking van sollicitaties via internet zonder menselijke tussenkomst. In drie gevallen is geautomatiseerde individuele besluitvorming wel mogelijk:
a. het is noodzakelijk voor de totstandkoming of de uitvoering van een overeenkomst;
b. het is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling;
c. het berust op de uitdrukkelijke toestemming van de betrokkene.

4.1.3 Toegang voor een ieder
Uitgangspunt is dat niemand toegang heeft tot persoonsgegevens tenzij er een grondslag voor bestaat. Deze grondslag zal te allen tijde direct moeten worden opgegeven indien erom gevraagd wordt. Let wel de bewijslast of iets mag ligt bij de gemeente.

4.1.4 Koppeling naar BIG
De BIG is de ene kant van de medaille, privacy de andere. Is de BIG niet op orde, dan is de privacy ook niet op orde. Een groot aantal referentienummers van de BIG heeft een directe werking op de mate van privacybescherming. Het privacybeleid moet dus nadruk gekoppeld worden aan de BIG.

4.1.5 Koppeling naar PIA
In de AVG is vastgelegd dat er voor elke nieuwe verwerking of wijziging van verwerking een PIA moet worden gedaan. Hiervoor is de FG toezichthouder, maar de uitvoering van dit beleid ligt bij de betreffende onderdelen van de organisatie. De leidinggevenden binnen de organisatie moeten worden toegerust om een PIA te maken.
De PIA's moeten in een centraal register samen met het register van verwerkingen en de verwerkersovereenkomsten worden ondergebracht.
Bij een vraag van een inwoner of de Autoriteit Personeelsgegevens zullen die gegevens per omgaande moeten kunnen worden geleverd.

gemeente Staphorst

Bijlage 1: De AVG en de Zelfredzaamheidsmatrix

De AP is van oordeel dat de verwerking van persoonsgegevens met behulp van de ZRM door de gemeente Zaanstad niet voldoet aan de zorgplicht van artikel 15 van de Wbp. Tevens is er ten aanzien van de verwerking van (bijzondere) persoonsgegevens die niet noodzakelijk zijn voor de toeleiding naar zorg op grond van de Wmo 2015 sprake van strijd met het vereiste van doelbinding van artikel 7 van de Wbp en het verbod op het bovenmatig verwerken van gegevens van artikel 11, eerste lid, Wbp.

Ook ontbreekt bij het verwerken van niet noodzakelijke (bijzondere) persoonsgegevens een uitzondering op het verbod op het verwerken van bijzondere persoonsgegevens van artikel 16 van de Wbp en een grondslag in artikel 8 Wbp dan wel artikel 5.1.1 van de Wmo 2015.

Daarnaast is er géén uitzondering in de Wbp of de Wmo 2015 voor het verwerken van strafrechtelijke gegevens voor de toeleiding naar zorg op grond van de Wmo 2015. Het verwerken van strafrechtelijke gegevens ten behoeve van het domein "Justitie" van de ZRM is voor de Wmo 2015 dan ook niet toegestaan.

Aldus wordt geresumeerd dat:

- Hoewel de gemeente Zaanstad voornemens is haar werkinstructies aan te passen is op dit moment in beleidsdocumenten en werkinstructies onvoldoende concreet uitgewerkt welke persoonsgegevens het wijkteam mag verwerken bij de toeleiding naar zorg, dat het functioneren van de cliënt alleen wordt geregistreerd ten aanzien van de gebieden waar hij problemen ervaart en waarvoor hij hulp behoeft en dat de professional onvoldoende is geëquipeerd om de beoordeling van de noodzaak van het registreren van gegevens te kunnen maken;
- Het geven van scores per leefgebied niet voldoet aan de vereisten van proportionaliteit en subsidiariteit omdat met minder persoonsgegevens kan worden volstaan bij het inzichtelijk maken van de hulpvraag van de cliënt en de toeleiding naar zorg;
- In een aantal dossiers leefdomeinen waren geregistreerd terwijl daarvoor geen noodzaak was. Daarmee was niet voldaan aan de vereisten van proportionaliteit en subsidiariteit;
- De gemeente Zaanstad heeft deze overtreding inmiddels beëindigd;
- Het opnemen van contactjournaals waarin volledige telefoongesprekken en/of e-mails met of over betrokkene zijn weergegeven risico meebrengt op niet noodzakelijke en bovenmatige verwerking van persoonsgegevens. De gemeente Zaanstad heeft laten weten op dit punt de werkinstructie te hebben aangescherpt.

Een uitgebreide rapportage van de AP over dit onderzoek is te vinden op de website van de Autoriteit Persoonsgegevens, onder *Rapport definitieve bevindingen z2016-11845* (15 februari 2018).

gemeente Staphorst

Bijlage 2 Voorbeeld toestemmingsformulier

De Autoriteit Persoonsgegevens heeft in dit rapport toegelicht dat toestemming doorgaans niet is vereist voor de verwerking van persoonsgegevens in het sociaal domein. Er zal dus niet vaak gebruik hoeven te worden gemaakt van toestemming als grondslag voor de verwerking van persoonsgegevens.

Het vragen van toestemming als grondslag voor gegevensverwerking is wel nodig als er geen andere grondslag voor de verwerking van persoonsgegevens is. In dat geval zal goed moeten worden nagegaan of deze toestemming voldoet aan de in bijlage I beschreven randvoorwaarden uit de Wbp. Het bijgevoegde voorbeeld toestemmingsformulier kan daar een hulpmiddel voor zijn.

Daarnaast kunnen elementen uit dit voorbeeld toestemmingsformulier ook worden gebruikt als toestemming nodig is als grond voor de doorbreking van de geheimhoudingsplicht van een hulpverlener in het sociaal domein. Met name om te waarborgen dat deze toestemming voor de doorbreking van de geheimhoudingsplicht voldoende specifiek is. Zowel voor wat betreft de aard en omvang van de gegevens die worden verstrekt als met betrekking tot de personen en instanties met wie gegevens worden uitgewisseld.

Voorbeeld toestemmingsformulier (toestemming als grondslag voor de verwerking van persoonsgegevens)

Met dit formulier geef ik .....Hulpverlener X..... van Wijkteam Y.....

toestemming om gegevens over mij te verwerken. Het kan gaan om gegevens over mij die door het wijkteam worden geregistreerd, gegevens die worden opgevraagd bij andere hulpverleners of instellingen of gegevens over mij die door het wijkteam worden verstrekt aan anderen.

Hieronder kruis ik voor welke gegevensverwerkingen ik toestemming geef.

<u>Ik geef toestemming onder deze voorwaarden:</u>

- Mijn toestemming geldt alleen voor de hieronder beschreven redenen, gegevens en personen / instellingen. Voor nieuwe gegevensverwerkingen vraagt het wijkteam mij opnieuw om toestemming;
- Het wijkteam informeert mij over de gegevens die over mij worden uitgewisseld en de gegevens die over mij worden geregistreerd. Dat betekent bijvoorbeeld dat het wijkteam mij uitlegt om welke specifieke gegevens het gaat en waarom deze gegevens noodzakelijk zijn om mij te kunnen helpen;
- Als gegevens niet (meer) noodzakelijk zijn zal het wijkteam deze niet registreren dan wel verwijderen;
- Ik kan ervoor kiezen om geen toestemming te geven of om alleen voor bepaalde delen toestemming te geven. Het wijkteam legt uit wat de gevolgen voor mijn hulpverlening zijn als ik (voor bepaalde) gegevens of personen geen toestemming geef;
- Ik mag mijn toestemming op elk moment intrekken. In sommige gevallen zal het intrekken van toestemming gevolgen hebben voor mijn hulpverlening. Het wijkteam zal mij hier van geval tot geval over informeren;
- Deze toestemming is een jaar geldig.

Gegevens over mij op te nemen in systeem Y Ja / Nee

Gegeven mogen over mij worden opgevraagd bij:

Instelling A

De gegevens

..... Ja / Nee

Deze gegevens zijn nodig omdat

.....

Instelling B

De gegevens

gemeente Staphorst

..... Ja / Nee

Deze gegevens zijn nodig omdat

.....

Instelling C

De gegevens

..... Ja / Nee

Deze gegevens zijn nodig omdat

.....

School

De gegevens

..... Ja / Nee

Deze gegevens zijn nodig omdat

.....

Huisarts

De gegevens

..... Ja / Nee

Deze gegevens zijn nodig omdat

.....

Medisch specialist

De gegevens

..... Ja / Nee

Deze gegevens zijn nodig omdat

.....

Gegevens mogen over mij worden verstrekt aan:

Instelling A

De gegevens

..... Ja / Nee

Deze gegevens zijn nodig omdat

.....

Instelling B

De gegevens

..... Ja / Nee

Deze gegevens zijn nodig omdat

Instelling C

De gegevens

…… Ja / Nee

Deze gegevens zijn nodig omdat

……

School

De gegevens

…… Ja / Nee

Deze gegevens zijn nodig omdat

……

Huisarts

De gegevens

…… Ja / Nee

Deze gegevens zijn nodig omdat

……

Medisch specialist

De gegevens

…… Ja / Nee

Deze gegevens zijn nodig omdat

……

Ik vind het goed dat mijn huisarts wordt geïnformeerd over het feit dat ik wordt geholpen door het wijkteam. Ja / Nee

Dit is nodig omdat……

Handtekening

……

Handtekening wettelijk vertegenwoordiger
(indien van toepassing)

……