Beleidsplan veilig omgaan met persoonsgegevens

Datum: 24 april 2018.

Burgemeester en wethouders,

R. Jager, burgemeester
N. Dusink, gemeentesecretaris

Inhoudsopgave

Bijlagen:

1. Inleiding

Artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden luidt:

Right to respect for private and family life
1 Everyone has the right to respect for his private and family life, his home and his correspondence.
2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Artikel 10 van de Grondwet luidt:
1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
2 De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
3 De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

In de Wet bescherming persoonsgegevens is verder uitwerking gegeven aan het grondrecht van eerbiediging van de persoonlijke levenssfeer. Het toezicht op de naleving van deze wet ligt bij de Autoriteit Persoonsgegevens. Door recente wetswijzigingen heeft de Autoriteit aan kracht gewonnen. Zo zijn de maximale boetebedragen die de Autoriteit kan opleggen sterk verhoogd en zijn organisaties die persoonsgegevens verwerken verplicht om datalekken te melden.

Inmiddels is bescherming van persoonsgegevens naar Europees niveau getild en geharmoniseerd. Op 25 mei 2016 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden en zullen verwerkingsverantwoordelijken (waaronder gemeenten) vanaf 25 mei 2018 geconfronteerd worden met handhaving door de Autoriteit Persoonsgegevens. De aspecten uit de Wet bescherming persoonsgegevens die betrekking hebben op het werk van de Autoriteit Persoonsgegevens zullen grotendeels worden overgeheveld naar de Uitvoeringswet Algemene Verordening Gegevensbescherming en voor het overige worden ingetrokken.

Dit beleidsplan geeft gemeentelijke invulling aan de AVG. Een belangrijk issue in de Verordening is het in lijn brengen van gemeentelijke taken waarbij persoonsgegevens worden verwerkt, het doel van de verwerking, de juridische grondslag voor de verwerking en de wijze waarop met een minimum aan persoonsgegevens het doel van de verwerking kan worden bereikt.

Voldoen aan de AVG betekent dat op verschillende terreinen binnen de gemeentelijke organisatie aandacht moet zijn voor privacy. Het toverwoord in de AVG is compliance. Bedrijven en overheidsinstanties moeten aantonen dat zij inspanningen hebben gedaan om aan de wet- en regelgeving te voldoen. Om die reden zullen governance, beleid, werkprocessen en triages, bewustwording en het beheer en opslag van gegevens onder de loep genomen worden die mogelijk leiden tot aanpassing van processen of werkafspraken.

In dit beleidsplan worden allereerst een aantal begrippen en het algemene kader voor gegevensverwerking besproken. Vervolgens zal dieper ingegaan worden in hoofdstuk 5 op beleid, governance in hoofdstuk 6, werkprocessen en triages in hoofdstuk 7, bewustwording in hoofdstuk 8 en tot slot in hoofdstuk 9 op beheer en opslag van persoonsgegevens.

Het beleidsplan is in samenwerking met de gemeenten Steenwijkerland en Zwartewaterland opgesteld. Waar van toepassing is ‘couleur locale’ toegepast, hetgeen wil zeggen dat de tekst van het beleidsplan op de Westerveldse situatie geënt is. De samenwerking heeft verder geleid tot het gezamenlijk aanstellen van functionarissen gegevensbescherming.

2. Samenvatting

Volgens de AVG is *het college van burgemeester en wethouders* verwerkingsverantwoordelijk en is zij gehouden aan de verordening te voldoen. Deze bestuurlijke verantwoordelijkheid zal voor de dagelijkse sturing worden belegd bij één collegelid.

In de praktijk is privacy een issue dat op de werkvloer speelt. Uitgangspunt in dit beleidsplan is om de verantwoordelijkheid zo dicht mogelijk bij de werkvloer te organiseren door het mandateren van taken en bevoegdheden aan de teamleiders Het mandaat behelst het geven van bevoegdheden en middelen om zelfstandig per team sturing te geven aan het privacybeleid.
De *concernadviseurs* (de CISO en de privacyofficer) en de toezichthouder (de functionaris gegevensbescherming) bieden ondersteuning bij het inrichten van de kaders, zijn adviseurs voor technische en organisatorische kwesties, hebben een coördinerende rol in de planning- en controlcyclus en verwerken datalekken.
De *teams* zijn verantwoordelijk voor het inrichten van de interne processen, het opstellen van de juiste documenten (protocollen, verwerkersovereenkomsten, etc.) en de archivering van persoonsgegevens.

De betrokkenheid van het college bij de vormgeving van het privacybeleid bestaat uit het jaarlijks vaststellen van een activiteitenplan bestaande uit privacybeleid en informatieveiligheidsbeleid, geldend voor de gehele organisatie en een verantwoording over de inzet van middelen en het resultaat in het voorafgaande jaar bevat.

De gemeente wil optimaal gebruik maken van de ruimte die de AVG biedt om persoonsgegevens te verwerken. Welke ruimte er precies is, ligt nog niet in beton gegoten. Daarom zal de gemeente binnen de lijnen van de verordening handelen, maar zal zij (als de situatie daar om vraagt) bereid zijn om risico te nemen om de grenzen van de verordening op te zoeken (bv door middel van triages).

3. Begrippen

In dit beleidskader worden verschillende begrippen geïntroduceerd met een zekere lading vanuit de privacy-wetgeving. Het gaat hierbij om:

- Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); 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;
- Bijzondere persoonsgegevens: alle persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de, unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemand seksueel gedrag of seksuele gerichtheid.
- Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
- Verwerkingsverantwoordelijke: 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;
- Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
- Bestand: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;
- Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;
- Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;
- Toestemming van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;

4. Algemeen kader voor de verwerking van persoonsgegevens

Gemeenten hebben van oudsher de beschikking over een veelheid aan persoonsgegevens. Met deze persoonsgegevens dient zorgvuldig te worden omgegaan. Vanuit de Algemene Verordening Gegevensbescherming (AVG) geldt de verplichting dat het verzamelen van persoonsgegevens steeds gekoppeld moet zijn aan een bepaald doel, de doelbinding. Binnen de gemeentelijke organisatie worden voor verschillende doelen persoonsgegevens verwerkt.

4.1 Doelbinding

Doelbinding
De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt.

Uitgangspunt in de AVG is de verwerking van de persoonsgegevens. Deze verwerkingen worden gedaan in het kader van de taakuitoefening door medewerkers. Voor deze verwerkingen geldt dat er een doel geformuleerd moet worden waarvoor zij worden verwerkt.
De AVG laat in het midden hoe die doelen geformuleerd worden, Uitgangspunt van de verordening is dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. De teamleider bepaalt in eerste instantie voor welke doelen zijn/haar team persoonsgegevens verwerkt, bijvoorbeeld vergunningverlening, subsidievaststelling of vaststellen hoogte uitkering. Deze doeleinden worden opgenomen in het register van verwerkingen. De functionaris gegevensbescherming die het register onder zich houdt toetst dit verder . In de praktijk wordt het toegestaan dat een doelomschrijving uit meerdere onderdelen bestaat, bijvoorbeeld in een constructie hoofddoel en subdoelen of nevendoelen. Van belang is daarbij dat deze doelstellingen onderling verenigbaar zijn. Het is ook mogelijk dat verwerkingen na melding voor andere doeleinden worden aangewend. Ook dit laatste is toegestaan, mits dit latere doel verenigbaar is met het oorspronkelijke.

Voor de gemeente betekent dat er zicht moet zijn op verwerkingsactiviteiten van medewerkers. Om die reden zal ter uitwerking van dit beleidsplan een verwerkingenregister worden opgesteld (welke ook verplicht is op grond van artikel 30 AVG). In dit register wordt de koppeling gelegd tussen de activiteiten van de gemeente en de persoonsgegevens die worden verwerkt. Aan de hand daarvan zal door de teamleider beoordeeld moeten worden of daar een gerechtvaardigd doel aan ten grondslag ligt (die uiteindelijk ook gemeld worden).
Een en ander kan betekenen dat er persoonsgegevens worden verwerkt waarvoor geen gerechtvaardigd doel is aan te geven. Dergelijke verwerkingen zullen worden beëindigd.

4.2 Dataminimalisatie

Dataminimalisatie
De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Voor alle afzonderlijke doelen dient vastgesteld te worden welke persoonsgegevens hiertoe noodzakelijkerwijs verwerkt moeten worden. Uitgangspunt is dat het verwerken van persoonsgegevens *toereikend, ter zake dienend* en *niet bovenmatig* mag zijn.
Toereikend wil zeggen dat op basis van de verwerking het juiste beeld gaat ontstaan. *Ter zake dienend* hangt nauw samen met het doel. *Bovenmatig* tot slot hangt ook samen met het doel.

Voor de gemeente geldt dat teams per verwerking moeten vaststellen welke persoonsgegevens ten minste noodzakelijk zijn om het doel te kunnen bereiken.

4.3 Vereisten van proportionaliteit en subsidiariteit

Proportionaliteit
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.
Subsidiariteit
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

Naast de hiervoor genoemde beperkingen voor verwerking van persoonsgegevens gelden ook de eisen van *proportionaliteit* en *subsidiariteit*.

Het *proportionaliteitsbeginse*l houdt in dat de inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Anders gezegd; hoe verhoudt het doel van de informatieverzameling zich tegenover de schending van de persoonlijke levenssfeer van de betrokkenen.
Ingevolge het *subsidiariteitsbeginse*l mag het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene, minder nadelige wijze kunnen worden verwerkelijkt (bv het verkrijgen van de informatie uit open data).

Ook hier zal per team door de gemeente Westerveld beoordeeld moeten worden of de verwerking doelmatig is, de inbreuk op de persoonlijke levenssfeer niet zwaarder weegt als de verwerking en of de persoonsgegevens ook op een andere wijze verkregen kunnen worden.

4.4 Grondslag

Grondslag
Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

Om persoonsgegevens te mogen verwerken is het noodzakelijk dat er een geldige grondslag is op basis waarvan de gegevens mogen worden verwerkt. Artikel 6 AVG geeft hiertoe een limitatieve opsomming:
- ondubbelzinnige toestemming,
- ter uitvoering van een overeenkomst,
- ter uitvoering van een wettelijke taak,
- ter vrijwaring van een vitaal belang,
- voor een goede vervulling van een publieke taak of van een taak in het kader van uitoefening openbaar gezag opgedragen aan de verwerkingsverantwoordelijke of
- vanuit gerechtvaardigde belangen (deze grondslag kan niet door overheidsinstanties gebruikt worden, tenzij deze overheidsinstanties optreden als privaatrechtelijke partij)

Voor de verwerking van de persoonsgegevens is het noodzakelijk dat aansluiting gevonden kan worden bij een van deze grondslagen. Hierbij kan worden aangetekend dat de eerste grondslag enkel gebruikt wordt (ondubbelzinnige toestemming) als op grond van een van de andere grondslagen geen persoonsgegevens kunnen worden verwerkt. Als op basis van een andere grondslag (voor de gemeente zal dit in de regel het uitvoeren van wettelijke taken of een goede vervulling van publieke taken zijn) het mogelijk is gegevens te verzamelen, dan wordt geen toestemming aan de betrokkene gevraagd, tenzij een wettelijke bepaling daartoe verplicht.

4.5 Verwerkingsverantwoordelijke(n) en verwerker

Delen met derden
In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. De gemeente gaat deze afspraken controleren.

In de AVG wordt onderscheid gemaakt tussen *verwerkingsverantwoordelijke* en *verwerker.*
De *verwerkingsverantwoordelijke* is de overheidsinstantie, dienst of ander orgaan die alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.
De *verwerker* is de overheidsinstantie, dienst of ander orgaan die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Voorbeelden van verwerkers zijn ICT-dienstverleners of organisaties bij wie de gemeente een aantal taken laat uitvoeren.

In de relatie verwerkingsverantwoordelijke en verwerker heeft laatstgenoemde geen zeggenschap over het doel en de middelen van de verwerking. Doel en middelen worden door de verwerkingsverantwoordelijke bepaald. Om te zorgen dat de verwerker zich richt naar de instructies van de verwerkingsverantwoordelijke en kan garanderen aan de verwerkingsverantwoordelijke dat het passende technische en organisatorische maatregelen heeft genomen om de rechten van betrokkenen te beschermen, wordt een verwerkersovereenkomst gesloten (zie bijlage 3). De wetgever laat het in het midden of dit een aparte overeenkomst moet zijn of dat deze geïncorporeerd kan worden in de overeenkomst tot opdracht of samenwerkingsovereenkomst. De gemeente kiest in nieuwe situaties voor het laatste, zodat afspraken over verwerken deel uitmaken van de algehele set van afspraken die partijen onderling maken. In bestaande situaties worden samenwerkingsovereenkomsten niet opengebroken.
Het template van de verwerkersovereenkomst van de gemeente is als bijlage 3 aan dit beleidsplan toegevoegd.

Het is ook mogelijk dat twee of meer verwerkingsverantwoordelijken gezamenlijk het doel en de middelen van de verwerking bepalen. In die gevallen is het van belang dat op een transparante wijze de onderlinge verplichtingen zijn vastgelegd. Voor de gemeente geldt dat als sprake is van een gezamenlijke verwerkingsverantwoordelijkheid dit vooraf is vastgelegd in een samenwerkingsovereenkomst aangevuld met het protocol gegevensbescherming (zie bijlage 2). Een voorbeeld waarbij persoonsgegevens van de ene verantwoordelijke naar de andere verantwoordelijke worden overgedragen is te vinden in hoofdstuk 5 van de Wet maatschappelijke ondersteuning waar zorginstellingen als zelfstandig verantwoordelijke worden genoemd.

4.6 Technische en organisatorische beveiliging

De verantwoordelijke legt passende technische en organisatorische maatregelen (vandaar het belang om privacybeleid en informatieveiligheidsbeleid integraal uit te voeren) ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.

In de gemeente wordt aan deze eis van passende maatregelen invulling gegeven door het invoeren van de maatregelenset van de Baseline Informatiebeveiliging Gemeenten (BIG). Deze baseline is ontwikkeld door VNG Realisatie. Met de implementatie van deze set worden de volgende zaken beoogd:

- het invoeren van een basisniveau van informatiebeveiliging: de set is zo opgezet en ingevuld dat met invoering van de maatregelen een passend beveiligingsniveau wordt gerealiseerd voor de meeste toepassingen. Deze maatregelen betreffen niet alleen ICT-technische maatregelen maar gaan ook over huisvesting, personeelsbeleid en -werving, contractmanagement, inkoop, voorlichting en bewustwording.
- het systematisch beoordelen van informatiesystemen en -verwerking op de beveiligings- en privacyrisico's en het zo nodig treffen van specifieke maatregelen bovenop het basis-beveiligingsniveau;
- het invoeren van een proces van plannen, uitvoeren, toetsen en bijsturen waarbij de maatregelenset systematisch gecontroleerd wordt op effectiviteit en zo nodig aangepast wordt om het passende beveiligingsniveau blijvend te kunnen waarborgen.

Het informatiebeveiligingsproces en de maatregelenset van de BIG wordt in verschillende varianten binnen de overheid gebruikt en zijn gebaseerd op de internationale beveiligingsstandaarden. ISO 270001 en ISO 270002.

4.7 Samenvatting

De eerste opdracht in het kader van de bescherming van persoonsgegevens is het bepalen van het aantal en de omvang van de verwerkingen die binnen de verschillende teams plaatsvinden.
Op teamniveau vaststellen:

- welke taken worden uitgevoerd en bepalen wat de doelen zijn van het team
- wat de grondslag van de verwerkingen is.
- dat aantal verwerkingen in bestanden worden vastgelegd (vast te leggen in het verwerkingenregister), In bijlage 4 is een invulformulier en een excellijst opgenomen welke gebruikt kan worden ten behoeve van individuele verwerkingen (al deze individuele verwerkingen vormen samen het verwerkingenregister).
- welke gegevens maximaal noodzakelijk zijn om de taak uit te kunnen oefenen.
- welke verwerkingen buiten de deur worden gedaan (en daar een verwerkersovereenkomst voor afsluiten). In bijlage 4 is een regel opgenomen waaruit blijkt of er sprake is van een verwerkersrelatie.
- de mandaatstructuur inzake verwerkersovereenkomsten.

5. Privacybeleid

De gemeente hecht er waarde aan dat de persoonsgegevens die aan haar zijn toevertrouwd alleen gebruikt worden voor de doeleinden waarvoor zij worden verwerkt. Deze bescherming van persoonsgegevens mag echter nooit een gevaar opleveren voor hulpverlening en veiligheid. In de AVG wordt een aantal generieke normen gesteld waaraan de verwerkingsverantwoordelijke inhoud moet geven. Door het normenkader zelf vorm te geven kan de verwerkingsverantwoordelijke eigen accenten aanbrengen of beleidsuitgangspunten toevoegen. De gemeente zoekt in dergelijke gevallen de grenzen van de privacywetgeving op als daarmee een groter gevaar kan worden afgewend dat kan ontstaan als medewerkers en andere hulpverleners langs elkaar heen werken. Beslissingen die in dat verband genomen worden zullen duidelijk gemotiveerd worden.

Het beleid van de gemeente is ook gericht op transparantie en bewustwording. Zowel intern als extern zal er een open communicatie zijn over de wijze van verwerking van persoonsgegevens.

Binnen het thema beleid verdienen vijf aspecten nadere invulling; rechten van betrokkenen, rechten personeelsleden, geautomatiseerde verwerkingen, datalekken en bewaren van persoonsgegevens.

5.1 Rechten van betrokkenen

Rechten van betrokkenen
De gemeente honoreert alle rechten van betrokkenen.

Binnen de AVG worden verschillende rechten toegekend aan betrokkenen opdat zij steeds de regie kunnen voeren op de persoonsgegevens die bij de gemeente worden verwerkt.
Het gaat om de volgende rechten:

1. Recht op informatie (artikel 12 AVG)
Er dienen maatregelen genomen te worden zodat de betrokkene op een beknopte, transparante, begrijpelijke en in gemakkelijk toegankelijke vorm informatie kan verkrijgen over zijn persoonsgegevens en geïnformeerd wordt over verwerkingsactiviteiten. Het verstrekken van informatie geschiedt onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek.

2. Recht op inzage (artikel 15 AVG)
Betrokkene heeft het recht uitsluitsel te krijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en om inzage te verkrijgen van die persoonsgegevens en de volgende informatie:
- verwerkingsdoelen,
- betrokken categorieën van persoonsgegevens,
- ontvangers of categorieën ontvangers aan wie persoonsgegevens worden verstrekt,
- duur van de verwerking en opslag,
- het recht op rectificatie en gegevenswissing,
- het recht om een klacht in te dienen bij de toezichthoudende autoriteit,
- (indien gegevens niet bij betrokkene worden verzameld) informatie over de bron van de gegevens en
- het bestaan van geautomatiseerde besluitvorming, het belang en de te verwachten gevolgen voor betrokkene.

3. Recht op rectificatie (artikel 16 AVG en 19 AVG)
Betrokkene heeft het recht dat onjuiste persoonsgegevens onverwijld worden gerectificeerd en dat onvolledige gegevens worden aangevuld. De verwerkingsverantwoordelijke stelt iedere ontvanger op de hoogte van de rectificatie of aanvulling.

4. Recht op gegevenswissing (artikel 17 AVG en 19 AVG)
Onder omstandigheden heeft betrokkene het recht dat zijn gegevens zonder onredelijke vertraging worden gewist. Per verwerking zal moeten worden bepaald of gegevenswissing mogelijk is. De verwerkingsverantwoordelijke stelt iedere betrokkene op de hoogte van de wissing.

5. Recht op beperking van de verwerking (artikel 18 AVG)
Onder omstandigheden heeft betrokkene het recht om een beperking van de verwerking te verkrijgen, indien de juistheid van de persoonsgegevens worden betwist, de verwerking onrechtmatig is, de persoonsgegevens niet meer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt of indien betrokkenen bezwaar heeft gemaakt tegen de verwerking

6. Recht op overdraagbaarheid (artikel 20 AVG)
Betrokkene heeft het recht om zijn persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en het recht deze gegevens over te dragen aan een andere verwerkingsverantwoordelijke.

7. Recht op bezwaar (artikel 21 AVG)
Betrokkene heeft steeds het recht bezwaar te maken tegen de verwerking. De verwerkingsverantwoordelijke staakt de verwerking, tenzij er dwingende gerechtvaardigde gronden zijn die zwaarder wegen dan de belangen van de betrokkene.

8. Recht om niet onderworpen te worden aan een enkel op geautomatiseerde verwerking gebaseerd besluit (artikel 22 AVG).
Betrokkene heeft het recht om niet onderworpen te worden aan een enkel op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.

9. Klachtrecht en schadevergoedingsrecht (artikel 77 AVG en artikel 82 AVG)
Betrokkene heeft het recht een klacht in te dienen bij de toezichthoudende autoriteit en het recht op een vergoeding van materiële of immateriële schade ten gevolge van inbreuk op bepalingen AVG en waarvoor de verwerkingsverantwoordelijke aansprakelijk is jegens de betrokkene.

Het uitgangspunt voor de gemeente is dat gestreefd wordt naar een maximale transparantie tegenover de betrokkene waar het gaat om de ‘eigen’ persoonsgegevens.
Waar het gaat om het recht op informatie zal de gemeente in zijn algemeenheid op de website en in de correspondentie betrokkenen wijzen op het feit dat de gemeente persoonsgegevens verwerkt en dat betrokkenen een aantal rechten hebben op grond van de AVG. Inhoudelijk worden deze verzoeken en bezwaren door de privacyofficer begeleid.

5.2 Rechten personeelsleden

In het licht van de AVG zijn de gegevens van medewerkers eveneens gegevens van betrokkenen en verdienen om die reden aandacht. Het is steeds gebruik geweest om namen van medewerkers te vermelden op uiteenlopende documenten. Deze documenten worden toegevoegd aan de college- of raadsagenda en worden langs die weg uiteindelijk in de openbaarheid gebracht. De vraag die voorligt is in hoeverre het zinvol is om de naam van medewerkers langs deze weg te openbaren. Al snel zal blijken dat er geen goede reden is te verzinnen waarom openbaar maken wenselijk is. Immers, medewerkers staan hoofdzakelijk (zo niet uitsluitend) ten dienste van het college van burgemeester en wethouders. In dat verband is het te billijken dat het college de naam van de behandelend ambtenaar te zien krijgt. Bij raadsstukken worden geen namen van medewerkers vermeld. Het stuk wordt aangeboden door het college (de publieke functie van het college impliceert reeds een vorm van toestemming om diens persoonsgegevens daarvoor te gebruiken).

In correspondentie naar burgers kan het persoonsgegeven van de medewerker genoemd worden, indien dit noodzakelijk is (bijvoorbeeld: welke Wmo-consulent gaat uw dossier behandelen). In die gevallen dat er geen noodzaak is persoonsgegevens van medewerkers te delen zal de naam van de medewerker worden vervangen door een alias (bv. eerste letter voornaam en de eerste drie letters achternaam). De medewerker kan zelf deze keuze maken.

In geval sprake is van Wob-verzoeken kunnen de namen van medewerkers achterwege blijven. Uit artikel 10, eerste lid onder d Wob vloeit dit al voort. Dit geldt echter niet voor ambtenaren die uit hoofde van hun functie in de openbaarheid treden. In het kader van dit beleidsplan wordt dit artikel gevolgd met de aanvulling dat er snel sprake zal zijn van een aantasting van de persoonlijke levenssfeer. Voor degene die Wob-verzoeken afhandelt betekent dit een extra alertheid.

5.3 Geautomatiseerde verwerkingen

Onder geautomatiseerde verwerkingen wordt verstaan het gebruikmaken van elektronische middelen om gegevens te verwerken. Een voorbeeld is profilering. Door het bezoeken van bepaalde gemeentelijke websites kunnen bepaalde persoonlijke aspecten worden vastgelegd en geanalyseerd en kan de gemeente aan de bezoeker bepaalde gerichte producten of diensten aanbieden. Hier maakt de gemeente geen gebruik van.

Belangrijke voorwaarden voor cameratoezicht door de gemeente zijn dat:
- andere maatregelen niet voldoende zijn gebleken om de openbare orde te handhaven

- inzet van camera's niet op zichzelf staat, maar in combinatie met andere maatregelen gebeurt (zoals betere straatverlichting of toezicht op straat
- de gemeente mensen informeert over het cameratoezicht (evt. met geluidsopnames), bijvoorbeeld met bordjes.
- de gemeente de camerabeelden niet langer dan 4 weken mag bewaren.

Voor onderzoeken zal de gemeente, indien dat in het kader van het onderzoek gewenst is, gebruik maken van Big data en tracking wanneer de aldus verzamelde gegevens niet te herleiden zijn tot een natuurlijke persoon. In die gevallen waarin de gemeente gebruik maakt van Big data onderzoeken en tracking, dan zal zij daarover vooraf informatie verstrekken op de gemeentelijke website.

5.4 Datalekken

Van een datalek is sprake bij een onrechtmatige verwerking en als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek is het gevolg van een beveiligingsincident. In de meeste gevallen gaat het om uitgelekte computerbestanden, al kan een verloren uitgeprinte klantenlijst evengoed een datalek vormen. Andere voorbeelden: cyberaanvallen (incl. DDos), e-mail verzonden naar verkeerde adressen, onderschepte e-mails, niet aangekomen post, gestolen laptops of bedrijfstelefoons, afgedankte niet-schoongemaakte computers en verloren usb-sticks.
Voor het melden van beveiligingsincidenten en datalekken is een procedure opgesteld.

5.5 Bewaren van persoonsgegevens

Bewaartermijn
Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwerking. Voor wat betreft het bewaren van persoonsgegevens gelden voor de gemeente twee regiems, het wettelijke regiem en het niet wettelijke regiem.
Voor sommige verwerkingen van persoonsgegevens geldt dat deze persoonsgegevens op grond van de Archiefwet of andere materiële wetten een minimale termijn bewaard moeten blijven. Een voorbeeld is het jeugdhulpdossier dat 15 jaar nadat de jeugdhulp beëindigd is bewaard moet blijven. De AVG gaat niet in op de wettelijke termijnen die bestaan of in de toekomst zullen ontstaan.
Voor die verwerkingen waarvoor geen wettelijke termijn geldt dat de verwerkte persoonsgegevens worden vernietigd zodra de verwerking niet meer noodzakelijk is ter bepaling door de teamleider en wordt vastgelegd in het verwerkingsregister welke bijgehouden wordt door de FG.

Voor wat betreft het archiveren van persoonsgegevens zoekt gemeente aansluiting bij artikel 89 AVG. Archiveren in het algemeen belang is mogelijk, mits passende maatregelen zijn getroffen om de betrokkenen te beschermen. Vaststaat dat persoonsgegevens die voor voor de behartiging van een publiek belang of een gerechtvaardigd doel zijn verwerkt ook verwerkt mogen worden in de zin van archiveren (verenigbaar doel). Wel zal men opnieuw moeten beoordelen of verdere dataminimalisatie mogelijk is. Is dataminimalisatie mogelijk door ontkoppeling van de persoonsgegevens met de overige gegevens, dan zal daar voor gekozen worden. Als tussenvorm is het mogelijk om in het kader van archivering te werken met pseudonimiseren.

5.6 Samenvatting

Uitgangspunt van beleid is dat niet alleen de persoonsgegevens van betrokkenen buiten de organisatie optimaal worden beschermd, maar ook die van het eigen personeel. In dit hoofdstuk komen daarom de rechten van betrokkenen maar ook van personeelsleden aan de orde. Er ligt inmiddels beleid hoe met datalekken om te gaan en zijn er maatregelen getroffen om persoonsgegevens waarvoor geen doel meer is aan te wijzen en waarbij geen wettelijke bewaarplicht geldt zo snel mogelijk te vernietigen.

6. Governance

Integriteit en vertrouwelijkheid
De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

Om te voldoen aan de AVG zullen op bestuurlijk en ambtelijk niveau binnen de gemeente een aantal organisatorische maatregelen noodzakelijk zijn. In paragraaf 6.1 en paragraaf 6.2 wordt de verdeling van bevoegdheden en verantwoordelijkheden geregeld tussen het bestuurlijk en ambtelijk niveau. Vanaf paragraaf 6.3 worden de functies benoemd die betrokken zijn bij het 'in control' brengen en houden van de gemeente.

6.1 Privacy op bestuurlijk niveau

Binnen de kaders van de AVG is het college bestuurlijk eindverantwoordelijk voor de verwerking van persoonsgegevens. Deze gezamenlijke verantwoordelijkheid wordt belegd bij één van de collegeleden die als vast aanspreekpunt fungeert voor privacy-issues. In de relatie met de gemeenteraad kiest de gemeente er voor de raad te informeren na vaststelling van dit beleidsplan.

Het college wil optimaal gebruik maken van de ruimte die de AVG biedt om persoonsgegevens te verwerken. Welke ruimte er precies is, ligt nog niet in beton gegoten. Dit betekent dat er een beleidsvrijheid is in het bepalen welke verwerkingen binnen de gemeente worden gedaan. Deze beleidsvrijheid wordt primair ingevuld door procesregisseurs. Onder omstandigheden kan het college uitdrukkelijk gevraagd worden in te stemmen met een verwerking. Het afwegingskader daarbij is de bescherming privacy burger afgezet tegen een eigen belang van de gemeente, bijvoorbeeld de veiligheid van de medewerkers.

Een ander aspect waarbij privacy op bestuurlijk niveau een rol speelt is het besluitvormingsproces. Het besluitvormingsproces van het college speelt zich grotendeels in de openbaarheid af. Deze openbaarheid kan gaan knellen op het moment dat er in documenten persoonsgegevens staan. Om die reden zullen persoonsgegevens zoveel mogelijk buiten collegebesluiten gehouden worden, tenzij de betrokkene toestemming heeft gegeven. Slechts in uitzonderlijke gevallen mogen persoonsgegevens zonder toestemming openbaar gemaakt worden.

Mocht het toch noodzakelijk zijn om persoonsgegevens in stukken op te nemen die bestemd zijn voor het college, dan zal vooraf een afweging worden gemaakt over de geheimhouding. Bij voorkeur is er een versie met persoonsgegevens waarop geheimhouding wordt opgelegd. In de openbare versie worden de persoonsgegevens dan onleesbaar gemaakt. Als dit niet goed mogelijk is dan kunnen de persoonsgegevens ook worden opgenomen in een geheime bijlage of kan zelfs het hele document geheim worden gehouden. Bedenk dat persoonsgegevens niet alleen hoeven te slaan op de inwoners van de gemeente, maar ook op medewerkers. Ook hun gegevens moeten zoveel mogelijk buiten verdere openbaring blijven.

Bij raadsstukken zijn alle stukken openbaar, tenzij er geheimhouding is opgelegd. Het beleid van de gemeente is er op gericht om geen persoonsgegevens in openbare stukken op te nemen, tenzij het een bewuste keuze is om het wel te doen.

6.2 Privacy op ambtelijk niveau

De feitelijke verwerking van persoonsgegevens vindt plaats binnen de ambtelijke organisatie op teamniveau. De uitwerking van de eindverantwoordelijkheid die het college draagt wordt ingevuld op dit niveau. Hier worden het doel en de middelen van de verwerking bepaald zoals gebleken is uit hoofdstuk 4. Het is niet meer dan logisch dat een deel van de bevoegdheden en verantwoordelijkheden op het terrein van de privacy die ligt bij het college gemandateerd wordt naar teamleiders, zodat zij op effectieve wijze privacy in hun dagelijkse processen kunnen incorporeren.

Langs deze weg worden teamleiders primair verantwoordelijk om passende technische en organisatorische maatregelen treffen om de rechten van betrokkenen te waarborgen en de verwerking in overeenstemming te brengen met de AVG. De technische maatregelen behelzen voornamelijk het organiseren van de autorisaties en het bepalen van het beveiligingsniveau. De organisatorische maatregelen hebben betrekking op het bewust omgaan met persoonsgegevens en het treffen voorzieningen waardoor medewerkers hun taken kunnen blijven uitvoeren.

De verantwoordelijkheid van de teamleider op privacygebied is gekoppeld aan mandaten vanuit het college met daarin bevoegdheden en middelen. Hierbij kan worden gedacht aan:
- inrichten van de werkprocessen in overeenstemming met AVG,
- bepalen van het doel en middel van de verwerking,
- alloceren middelen in termen van menskracht en geld voor onder andere bewustwordingssessies,
- bepalen van (mede)verantwoordelijkheid voor de verwerking,
- voorbereiden van verwerkingsrelaties, protocollen en verwerkersovereenkomsten opstellen (al dan niet als onderdeel van de samenwerkingsovereenkomst),
- technische infrastructuur voor de verwerkingen,
- archivering,
- inzetten privacy impact assessment (PIA) of soortgelijke instrumenten om de privacy te toetsen,
- waarborgen rechten betrokkenen,
- melden van verwerkingen bij de functionaris gegevensbescherming (FG) en
- melden datalekken en andere incidenten

De teamleiders dragen er ook zorg voor dat medewerkers in de teams gehouden zijn tot geheimhouding van de persoonsgegevens waar zij kennis van nemen. Voor de ambtenaren die reeds in vaste dienst zijn bij de gemeente geldt de eed of gelofte. Voor nieuwe medewerkers geldt aanvullend dat direct op de eerste werkdag een geheimhoudingsverklaring ondertekend wordt.
Voor personen die niet in dienst zijn van de gemeente (bijvoorbeeld leden van de bezwarencommissie) of die tijdelijk worden ingehuurd geldt dat zij eveneens een geheimhoudingsverklaring moeten tekenen.
Het template van de geheimhoudingsverklaring is opgenomen in bijlage 1.

6.3 Functionaris gegevensbescherming

Op grond van artikel 37 AVG wordt een functionaris gegevensbescherming (FG) aangewezen. De verwerkingsverantwoordelijke draagt hierbij zorg dat de FG aangewezen wordt op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen om de taken die met zijn functie samenhangen, genoemd in artikel 39 AVG, te vervullen.

De verwerkingsverantwoordelijke is op grond van artikel 37 AVG gehouden om de contactgegevens van de FG bekend te maken en mede te delen aan de Autoriteit Persoonsgegevens (AP). Binnen de gemeente Westerveld valt de FG formatief onder het team Bedrijfsvoering

De FG is primair toezichthouder en heeft een informerende en adviserende rol aan de organisatie over verplichtingen die voortvloeien uit de verordening. Daarnaast ziet de FG toe op de naleving van de verordeningsbepalingen en draagt de functionaris zorg voor de privacy-audits. Tot slot fungeert de FG als eerste aanspreekpunt voor de Autoriteit Persoonsgegevens.

Van resultaten uit audits en overige bevindingen doet de FG rechtstreeks verslag aan het college van burgemeester en wethouders.

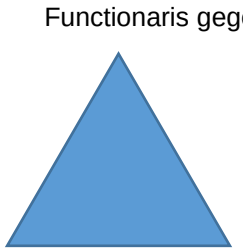
6.4 Coördinator rechtsbescherming

In geval van een schending dan wel uitoefening van rechten van betrokkenen (zie paragraaf 6.1) moet een betrokkene, los van andere juridische middelen, zich kunnen wenden tot de gemeente als verwerkingsverantwoordelijke.

Binnen de gemeente is een coördinator aangewezen waar verzoeken en bezwaren (ex artikel 21 AVG) kunnen worden ingediend. De coördinator bewaakt de termijn en draagt er zorg voor een goede afhandeling van het verzoek of bezwaar. De termijn voor het afhandelen van een klacht bedraagt maximaal 4 weken. Deze functie is belegd bij de privacyofficer.

6.5 Overige functies in het kader van de privacy
Buiten de in de AVG met naam genoemde functie van FG houden zich binnen de gemeente Westerveld ook anderen zich nadrukkelijk bezig met de dagelijkse praktijk rond privacy.

Organisatorisch wordt op twee niveaus uitwerking gegeven aan het privacybeleid; concern- en teamniveau. Op concernniveau vertaalt het zich in een driehoek bestaande uit FG, CISO en een privacyofficer (PO).



Naast toezicht op naleving AVG ziet de FG samen met de controller informatiebeveiliging tevens toe op informatieveiligheid, waarmee er op het gebied van informatieveiligheid een goede functiescheiding is gemaakt. De CISO zorgt er voor dat de juiste en passende beveiligingsmaatregelen gekozen, geïmplementeerd en geëvalueerd worden. De FG ziet toe op de werking van het proces en de maatregelen en brengt hier verslag van uit aan het management en bestuur.

Binnen de gemeente is de PO verantwoordelijk voor het vormgeven en actualiseren van het gemeentelijke privacy-beleid, het doen van organisatorische aanpassingen en draagt hij zorg dat documenten en andere beslissingen voldoen aan de privacywetgeving. Tot slot fungeert de PO als aanspreekpunt voor vragen over toepassing wet- en regelgeving inzake privacy.

De CISO heeft vooral tot taak om de veiligheidsorganisatie verder vorm te geven (hier valt bescherming persoonsgegevens ook onder). De veiligheidsorganisatie ziet vooral toe op ICT-maatregelen en omgaan met vertrouwelijke informatie (waarbij persoonsgegevens een extra druk leggen op die vertrouwelijkheid). In het kader van vertrouwelijkheid van informatiedeling organiseert de CISO onder meer de autorisatiesschema's, toegang tot (vertrouwelijke) informatie, informatieveiligheid en de organisatorische maatregelen daaromtrent.

6.6 Externe relaties - verwerkersovereenkomst

Het verwerken van persoonsgegevens is geen doel op zich, maar zal steeds in het teken staan van een ander gerechtvaardigd doel dat met die verwerking zal worden bereikt (het verlenen van zorg, het houden van toezicht of het uitbetalen van salarissen). Ten behoeve van dat andere doel zullen vaak persoonsgegevens van elders betrokken worden of zullen persoonsgegevens worden overgedragen aan anderen.

Bij het verwerken van persoonsgegevens elders worden in de AVG twee mogelijke samenwerkingsconstructies genoemd; gezamenlijke verwerkingsverantwoordelijkheid en de verwerking namens de verwerkingsverantwoordelijke. Buiten deze twee in de AVG genoemde samenwerkingsconstructies is ook nog denkbaar dat de persoonsgegevens die door de gemeente worden verwerkt worden overgedragen naar een andere verwerkingsverantwoordelijke (denk bij het sociaal domein aan een zorginstelling waarbij de overdracht aan de andere verwerkingsverantwoordelijke bij wet geregeld is).

A. gezamenlijke verwerkingsverantwoordelijkheid
Van een gezamenlijk verwerkingsverantwoordelijkheid is sprake wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen. In dat geval stellen zij op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van hun verplichting uit hoofde van de AVG vast, met name met betrekking tot de uitoefening van rechten van betrokkenen en het verstrekken van informatie aan hen. De relatie tussen de verwerkingsverantwoordelijken onderling wordt bestendigd door middel van een protocol. In bijlage 2 bij dit beleidsplan is een voorbeeldprotocol gevoegd.

B. verwerkingsverantwoordelijke en verwerker
Wanneer een verwerking namens een verwerkingsverantwoordelijke wordt verricht, en de verwerker geen zeggenschap heeft over doel en middel van de verwerking, dan doet de verwerkingsverantwoordelijke uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking voldoet aan de eisen van de AVG.

De gemeente blijft als verwerkingsverantwoordelijke (mede-)aansprakelijk voor de geschonden rechten van betrokkenen door nalatigheden van de kant van de verwerker. Om de verantwoordelijkheid en aansprakelijkheden goed uit elkaar te houden zal de gemeente in deze situaties gebruik maken van verwerkersovereenkomsten. Het gebruik van verwerkersovereenkomsten is een verplichting die voortvloeit

uit de AVG. De verwerkersovereenkomst is vormvrij en kan dus ook geregeld worden in de bovenliggende overeenkomst tot samenwerking, opdracht, dienstverlening etc. Om een beeld te hebben van de wijze waarop de relatie tussen verwerkingsverantwoordelijke en verwerker moet worden vormgegeven is een template verwerkersovereenkomst als bijlage 3 bij dit beleidsplan opgenomen.

C. Overdracht van persoonsgegevens aan een andere verwerkingsverantwoordelijke
Daar waar het gaat om een overdracht van de persoonsverwerking (bijvoorbeeld in de vorm van bestanden) aan een andere verwerkingsverantwoordelijke zal er na overdracht geen gebondenheid meer zijn van de gemeente Westerveld. De inspanning van de gemeente blijft hier beperkt tot het vaststellen of de ontvangende partij daadwerkelijk verwerkingsverantwoordelijke is. (Een dergelijk situatie doet zich vaak voor in het sociaal domein waar zorginstellingen, SVB, AMHK in de wet als verwerkingsverantwoordelijke zijn aangewezen). Ook in deze situatie is het overdrachtsprotocol als genoemd in bijlage 2 een passende oplossing.

In hoofdstuk 4.5 is reeds aangegeven dat een verwerkersovereenkomst wordt afgesloten om te zorgen dat de verwerker zich richt naar de instructies van de verwerkingsverantwoordelijke en kan garanderen aan de verwerkingsverantwoordelijke dat het passende technische en organisatorische maatregelen heeft genomen om de rechten van betrokkenen te beschermen. De wetgever laat het in het midden of dit een aparte overeenkomst moet zijn of dat deze geïncorporeerd kan worden in de overeenkomst tot opdracht of samenwerkingsovereenkomst. De gemeente kiest in nieuwe situaties voor het laatste, zodat afspraken over verwerken deel uitmaken van de algehele set van afspraken die partijen onderling maken. In bestaande situaties worden samenwerkingsovereenkomsten niet opengebroken

6.7 Samenvatting

Bescherming van persoonsgegevens speelt zich af binnen de gehele gemeentelijke organisatie en op ieder gewenst niveau. De verantwoordelijkheid voor persoonsgegevens ligt bij het bestuur, terwijl de verwerking van persoonsgegevens op een veel lager niveau plaatsvindt. Uitgangspunt in dit beleidsplan is om de privacybescherming daar te organiseren waar de beslissingen worden genomen om tot verwerking over te gaan. Een logisch uitvloeisel daarbij is om de bevoegdheidstoedeling te laten vergezellen van het beleggen van verantwoordelijkheid op datzelfde niveau. Op concernniveau zullen vervolgens (al dan niet op grond van de AVG verplicht) een aantal taken worden belegd die betrekking hebben op het optimaal ondersteunen van de organisatie en de medewerkers die in de dagelijkse praktijk persoonsgegevens verwerken.

7. Werkprocessen

Wanneer inwoners meerdere (aan)vragen hebben op meerdere gebieden, dan wil je dit als gemeente het liefst in samenhang benaderen. Het afhandelen van het één kan immers gevolgen hebben voor het afhandelen van het ander. Als je zaken effectief én efficiënt wil afhandelen dan moet je integraal aan de slag. Daarom werken we binnen onze gemeente ook zaakgericht, om meer samenhang en verbinding tussen de gemeentelijke processen te creëren plus een integraal klantbeeld. En binnen het sociaal domein zorgt integraal werken juist voor minder verschillende hulpverleners en instanties over de vloer.
In dit hoofdstuk staat de vraag centraal op welke wijze de gemeente de (integrale) verwerking van persoonsgegevens vorm geeft in bedrijfsprocessen en op welke wijze medewerkers gebruik kunnen maken van databases.
In 7.1 zal het kader geschetst worden hoe verwerking van persoonsgegevens in de bedrijfsprocessen moet worden ingebed.
In 7.2 wordt een bijzondere toepassing van verwerking van persoonsgegevens besproken waar hulpverleners en veiligheidsadviseurs mee te maken hebben in de dagelijks praktijk.
Hoofdstuk 7.3 gaat dieper in op triages die hoofdzakelijk voorkomen in het sociaal domein.
Hoofdstuk 7.4 bespreekt het gebruik van BSN-nummers (een bijzonder persoonsgegevens op grond van de Uitvoeringswet AVG).
In 7.5 wordt dieper ingegaan op het verwerkingenregister dat door de gemeente moet worden aangelegd en op basis waarvan de FG zijn toezicht kan effectueren. In de laatste paragraaf wordt besproken hoe met Privacy Impact Assessments (PIA's) privacyrisico's van gegevensverwerkingen in beeld gebracht worden en hoe deze vervolgens te vertalen in het werkproces.

7.1 Inbedding in primaire processen

De AVG eist dat voor verwerking van persoonsgegevens de beginselen inzake verwerking van persoonsgegevens in acht genomen zijn. Deze beginselen vloeien voort uit artikel 5 en 6 AVG.

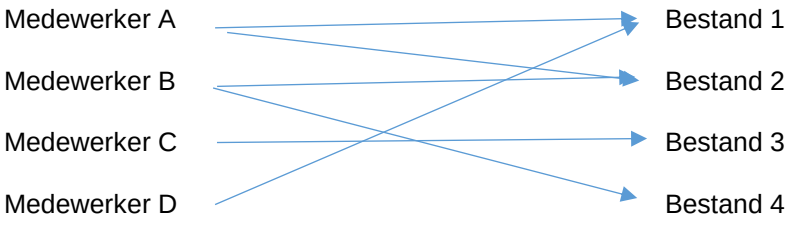
Zo moet de verwerking van persoonsgegevens kunnen steunen op *welbepaalde*, *uitdrukkelijk omschreven* en *gerechtvaardigde* doeleinden. Voor werkprocessen binnen de gemeente Westerveld betekent dit dat bij verwerkingen een geldige reden moet zijn om de inperking van het grondrecht privacy te rechtvaardigen. Ontbreekt een dergelijke reden, dan is de verwerking onrechtmatig en zal zij moeten worden beëindigd.

Concreet betekent een en ander dat er zicht moet zijn op de taken van (groepen) medewerkers waarbij persoonsgegevens worden verwerkt. Aan de hand van het overzicht van gegevensverwerkingen van de medewerkers zullen door de teamleiders gerechtvaardigde doeleinden moeten worden geformuleerd om de verwerking voort te kunnen zetten. Nadat doeleinden zijn geformuleerd is het noodzakelijk om te beoordelen welke persoonsgegevens ten minste verwerkt moeten worden om dat doel te kunnen bereiken. Persoonsgegevens die bovenmatig zijn kunnen buiten de verwerking blijven.

De volgende stap is dat aansluiting gevonden wordt bij een van de grondslagen uit artikel 6 AVG (zie tevens paragraaf 4.4). Voor de gemeente zal gaan gelden dat veel verwerkingen als grondslag de goede vervulling van een publieke taak kennen. In bijzondere gevallen zal een beroep op een van de andere grondslagen mogelijk of, in geval van toestemming, nodig zijn.

Uitgangspunt zijn de taken die door de medewerkers worden uitgevoerd. Deze taken vloeien voort uit functieomschrijvingen. Om in bestanden verwerkingen uit te kunnen voeren zal men toegang tot die bestanden moeten hebben door middel van autorisatie (waar het om digitale bestanden gaat). Het is belangrijk om steeds meerdere mensen te autoriseren voor dergelijke bestanden om te voorkomen dat een situatie ontstaat dat niemand bij de bestanden kan. Het is niet aannemelijk dat de teamleider per definitie toegang moet hebben, dit is ook weer afhankelijk van zijn takenpakket.

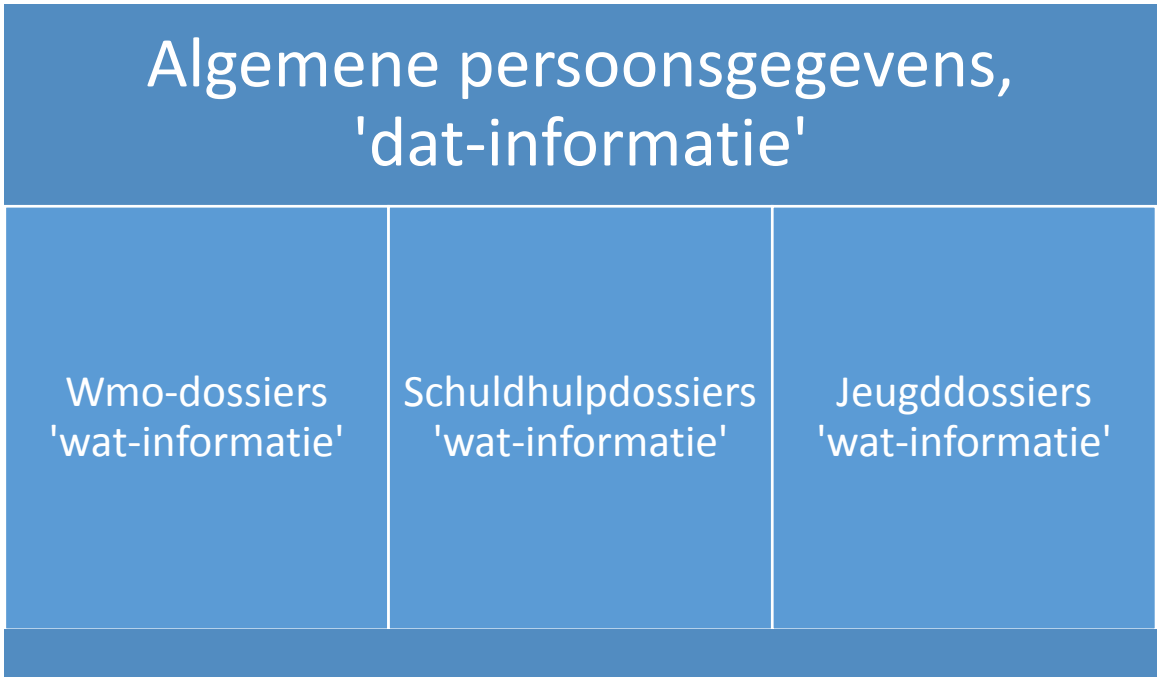
Schematische weergave:



7.2 Samenwerken met collega's

Binnen de gemeentelijke organisatie hebben medewerkers een takenpakket die bepalend is voor de toegang tot bestanden. Binnen takenpakketten kan er wel een onderscheid zijn in de diepte waarmee men toegang moet hebben tot de bestanden. Met name in het sociaal domein (mogelijk ook elders) kan het wenselijk zijn dat veel medewerkers een kleine hoeveelheid persoonsgegevens kunnen inzien en dat vervolgens een paar medewerkers de totale omvang van de persoonsgegevens (vastgelegd in bv een dossier) mogen inzien.

Deze werkwijze van zoveel mogelijk ondersteunen en tegelijkertijd binnen de grenzen van de privacywetgeving te blijven, vraagt om aanpassingen van het fundament. Denk aan:
- het minimaliseren van het tonen en gebruik van BSN nummer: overheidsorganisaties mogen het BSN nummer alleen gebruiken om hun taak uit te voeren als dit BSN nummer ook daadwerkelijk noodzakelijk is.
- onderscheid maken in "dat" en "wat" informatie en autorisatie hier op inrichten. De "dat" informatie maakt bijvoorbeeld inzichtelijk dát iemand een bepaalde aanvraag heeft lopen en kan breed toegankelijk zijn. De "wat" informatie is de inhoudelijke informatie die alleen toegankelijk is voor specifiek daartoe geautoriseerde personen.



7.3 Triage

Aparte aandacht verdient het proces rond de triage. Uitgangspunt in hulpverlening is om zoveel mogelijk te handelen vanuit 1 Gezin,1 Plan,1 Regisseur (1G1P1R). Triage speelt op casusniveau en vraagt van de medewerker om een professionele inschatting te maken wat de ernst van de problematiek is en welke verwerking van persoonsgegevens daarbij wenselijk is. Met name bij een multi-probleemsituaties in het sociaal domein kan er opschaling nodig zijn waardoor meer persoonsgegevens worden verwerkt of persoonsgegevens met anderen worden gedeeld. Dit is te rechtvaardigen om te voorkomen dat privacy in de weg gaat staan aan een effectieve hulpverlening. Triage maakt aldus de 1G1P1R-gedachte mogelijk.

Medewerkers bepalen per casus het doel waarvoor de gegevensverwerking noodzakelijk is voor optimale hulp. Daarnaast bepalen zij of er niet bovenmatig gegevens worden verwerkt of dat gegevens niet op een andere, minder ingrijpende wijze, kunnen worden verwerkt. Van belang is dat deze afweging door de medewerker wordt vastgelegd. Triagemomenten worden benoemd in het werkproces. De grondslag voor triage is voor de gemeente het uitvoeren van een publiekrechtelijke taak. Dit betekent concreet dat het toepassen van triage beperkt is tot die werkprocessen waarbij het uitwisselen van persoonsgegevens binnen en buiten de eigen organisatie terug te voeren is op het uitvoeren van een dergelijke taak. Medewerkers van Westerveld moeten er daarbij rekening mee houden dat het delen met professionele hulpverleners samenhangt met diens geheimhoudingsplichten (en dus niet alle gedeeld kan worden)

7.4 Gebruik burgerservicenummers

Er is nog veel onduidelijkheid over het gebruik van het BSN in werkprocessen. De regel is dat overheidsorganisaties het BSN mogen gebruiken om hun taak uit te voeren, mits het BSN hierbij noodzakelijk is. Organisaties buiten de overheid mogen het BSN alléén gebruiken als dit in de wet staat. En dan nog alleen voor de doelen die in de wet staan, dus niet zomaar overal voor.
Zo liet een kinderdagverblijf ouders inloggen op een online ouderportaal met hun BSN. Dat mag niet. Kinderdagverblijven mogen weliswaar naar het BSN van ouders vragen, maar zij mogen dit vervolgens alleen gebruiken voor de kinderopvangtoeslag.

Het voorbeeld van het kinderdagverblijf komt ook regelmatig terug in gemeentelijke processen. Zo mag de gemeente een BSN niet gebruiken als briefkenmerk of dossiernummer. De gemeente mag ook niet standaard om BSN vragen of laten vermelden in brieven die naar de gemeente gestuurd worden.

7.5 Verwerkingenregister

Zoals in het hoofdstuk Governance reeds is aangegeven ligt de ambtelijke verantwoordelijkheid voor het verwerken van persoonsgegevens bij de teamleiders. Zij brengen in beeld en bewaken het overzicht van de gegevensverwerkingen die binnen de teams plaatsvinden. Een voorbeeldformulier voor elke verwerking die op de afdeling plaatsvindt is toegevoegd in bijlage 4. Alle formulieren tezamen worden in een register ondergebracht.
Kader van het overzicht wordt gevormd door artikel 30 van de AVG. Zo zal onder meer vastgesteld moeten zijn dat de verwerking een gerechtvaardigd doel kent en gebaseerd is op een rechtmatige grondslag. Uiteindelijke levert dit het volgende plaatje op:

Verwerkingsregister									
Taakverantwoordelijke	Naam verwerking/proces	Doel verwerking	Betrokkenen	Persoonsgegevens	Bijzondere persoonsgegevens	Ontvangers	Grondslag	Bewaartermijnen	Beschrijving beveiligingsmaatregelen

Het overzicht van gegevensverwerkingen wordt geleverd aan de FG die gaat over toezicht op alle verwerkingen genoemd in het register.

7.6 Privacy Impact Assessment

Met het uitvoeren van een Privacy Impact Assessment (PIA) wordt inzicht verkregen in de privacyrisico's van een nieuwe dienst of een nieuw product. Maar ook het hergebruik van reeds verwerkte data voor nieuwe toepassingen is een voorbeeld waarvoor een PIA een duidelijk inzicht geeft aan de betrokken risico's.

Een PIA wordt bij voorkeur in een zo vroeg mogelijk stadium van het ontwerpproces uitgevoerd, zodat uitkomsten van de PIA nog meegenomen kunnen worden en invulling gegeven kan worden aan 'privacy by design'. Een PIA kan ook in een later stadium uitgevoerd worden, omdat de meeste processen doorontwikkeld worden en ook later nog privacyrisico's kunnen worden ingedamd.

Het is niet noodzakelijk om voor alle processen waarbij persoonsgegevens worden verwerkt een PIA uit te voeren. Om die reden is er een onderscheid aangebracht en zullen in 2018 enkel PIA's worden uitgevoerd in geval van nieuwe verwerkingen van persoonsgegevens en verwerkingen waarbij sprake is van een grote verzameling van persoonsgegevens of een verzameling met bijzondere categorieën van persoonsgegevens. Een selectie van verwerkingen waarvoor een PIA wordt georganiseerd vloeit voort uit het verwerkingenregister als genoemd in paragraaf 7.3.

De PIA's zullen onder leiding van de CISO worden uitgevoerd. Door de PIA gezamenlijk uit te voeren (een PIA bestaat uit een vraag-antwoordreeks) met vakspecialisten, systeembeheerders, PO en FG ontstaat er een leermoment voor delen van de organisatie.

Voor een aantal verwerkingen van persoonsgegevens zullen al voor 25 mei 2018 PIA's zijn/worden uitgevoerd. Om op juiste wijze PIA's uit te voeren, zal een gerichte training en opleiding worden verzorgd aan medewerkers die na 25 mei 2018 PIA's als begeleider gaan uitvoeren.

7.7 Samenvatting

De inhoud van de AVG dient zich te vertalen naar werkprocessen en daarnaast naar de dagelijkse omgang met persoonsgegevens. Hierbij is het noodzakelijk dat er zicht komt op alle verwerkingen binnen de

organisatie en dat er een overzicht is van het takenpakket van medewerkers, zodat op basis van taken die door de medewerker wordt uitgevoerd de toegang tot de bestanden met persoonsgegevens kan worden georganiseerd.
Verder wordt aandacht geschonken aan het uitvoeren van een PIA.

8. Bewustwording

8.1 Privacyveilig werken

Het is belangrijk dat privacy niet alleen leeft bij een aantal ‘ingewijden’, maar breed uitgedragen wordt binnen de organisatie. Dit vraagt om een interne bewustwording hoe omgegaan moet worden met de belangen van personen die persoonsgegevens aan de gemeente Westerveld hebben toevertrouwd, dit in combinatie met bewustwording over informatiebeveiliging in zijn algemeenheid.

Om bewust te blijven van de risico’s en de schade die kan ontstaan door informatiebeveiliging en gegevensbescherming niet serieus te nemen is een continue communicatie met betrekking tot deze onderwerpen nodig. Binnen de kaders van de gemeente Westerveld is in de aanloop naar 25 mei 2018 veel aandacht gegeven aan het bewustwordingsproces. Na 25 mei 2018 zal dit met regelmatige acties verder onder de aandacht blijven.

8.2 Bewustwording in de aanloop naar 25 mei 2018

Binnen de gemeente Westerveld is vóór 25 mei 2018 door de kwartiermaker FG al volop aandacht gegeven aan het thema privacy. De bewustwordingsacties volgden de voortgang van het beleidsproces. De bewustwording is opgebouwd rond drie thema’s: begrippen in de AVG, inhoud van het beleidsplan en betekenis van de AVG voor het dagelijks werk. Na 25 mei 2018 zullen met regelmatig vervolgacties zijn met daarin relevante actualiteiten.

Door kritisch na te denken over alle aspecten die samenhangen met de verwerking, zoals omvang en doel van de verwerking of de technische infrastructuur krijgen medewerkers inzicht in de kaders die gesteld worden aan een goede bescherming van persoonsgegevens.

Dit beleidsplan zal ook een bron vormen voor communicatie naar de teams. De gemeentelijke kaders in dit beleidsplan zullen met het collegelid en het college worden besproken en separaat met de teams. De gemeente stelt zich als doel om jaarlijks een activiteitenplan ‘privacy en informatieveiligheid’ op te stellen met daarin aandacht voor bewustwording en gegevensbeveiliging. Om de aandacht voor deze thema’s optimaal vast te houden is het de wens om dit plan steeds te laten vergezellen van een populaire versie die breed gecommuniceerd wordt binnen en buiten de gemeentelijke organisatie.

8.3 Bewustwording door teamactiviteiten

Uitgangspunt van het jaarlijkse activiteitenplan is om het bewustwordingsproces zo dicht mogelijk bij de medewerkers te organiseren. Welke communicatiemiddelen en trainingen worden ingezet ligt bij de teamleiders (met ondersteuning van concernadviseurs).

8.4 Samenvatting

Om de bewustheid voor het thema privacy vast te houden zal er jaarlijks geïnvesteerd moeten worden in privacy-bewustzijn. De uiteindelijke vormgeving hiervan ligt vast in jaarlijkse activiteitenplannen en waarbij zoveel mogelijk aansluiting wordt gezocht bij de activiteiten uit het informatieveiligheidsplan. Waar mogelijk worden beide thema’s gelijk opgetrokken.

9. Beheer en opslag van persoonsgegevens

9.1 Opslag van persoonsgegevens

Persoonsgegevens worden binnen de gemeente Westerveld (vrijwel) altijd digitaal opgeslagen. De manier waarop ons netwerk en gegevens zijn beveiligd dient in overeenstemming met de gemeentelijke beveiligingsnormen (BIG, zie ook 4.6) te zijn. Hiertoe dienen technische en organisatorische maatregelen getroffen te zijn. Mede in het licht van de uitvoering van het eerder vastgestelde Informatiebeveiligingsbeleid worden in 2018 maatregelen getroffen om informatiesystemen en opslag van data AVG-proof te maken.

9.2 Toegang tot en beheer van persoonsgegevens

Alleen geautoriseerde personen hebben toegang tot het netwerk van Westerveld en daarmee tot persoonsgegevens. Deze toegang tot het netwerk is beperkt tot applicaties en bestanden die vanuit de functie van de betrokkene noodzakelijk zijn. Voor toegang tot gestructureerde persoonsgegevens in centrale databases geldt een fijnmaziger toegang tot op specifiek gegevensniveau. Dit gebeurt op basis van rollen waarbij per medewerker of per functie een of meerdere rollen worden toegekend. Achter deze rollen hangt een autorisatieschema waarbij per type persoonsgegeven is vastgelegd in hoeverre deze vanuit de rol ingezien en veranderd mag worden. De toewijzing van rollen aan medewerkers wordt vastgelegd in autorisatiematrices en periodiek gecontroleerd.

De benodigde toegangsrechten worden vastgesteld door de teamleiders. Zij zijn verantwoordelijk voor de verwerking van persoonsgegevens (zie ook paragraaf 5.3) het beheer van de daarvoor benodigde applicaties en voor het treffen van afdoende beveiligingsmaatregelen. Het beheer van applicaties, en de daarin opgenomen persoonsgegevens en het daadwerkelijk toewijzen en inrichten van de toegangsrechten wordt uitgevoerd door applicatiebeheerders. De gemeente heeft hier een formele procedure.
Toegang tot persoonsgegevens wordt op gegevens- en medewerkersniveau geregistreerd (gelogd). Op deze manier is te achterhalen wie op welk tijdstip welke gegevens heeft geraadpleegd. Westerveld kent procedures om deze login te gebruiken bij privacyincidenten.

9.3 Samenvatting

Om de toegang en het beheer van persoonsgegevens in goede banen te leiden en te houden is het van belang dat persoonsgegevens zoveel mogelijk in robuuste datasystemen worden opgeslagen en dat het gebruik van eigen bestanden (al dan niet in papiervorm) zo veel mogelijk wordt ontmoedigd. Door gegevens zoveel mogelijk te verwerken in een centrale database kan de gemeente hierop haar beveiligingsmaatregelen optimaal inzetten. Bovendien maken centrale databases het beter mogelijk om het autorisatieschema er op in te richten, zodat onrechtmatige verwerkingen door medewerkers worden voorkomen.

Bijlage 1 Geheimhoudingsverklaring

GEHEIMHOUDINGSVERKLARING

De gemeente Westerveld hecht waarde aan een goede naleving van de privacywetgeving. Door ondertekening van deze privacyverklaring kunnen persoonsgegevens die door de gemeente Westerveld in het kader van de uitoefening van zijn taken worden verwerkt met u worden gedeeld.

De ondergetekenden:

Het college van burgemeester en wethouders van de gemeente Westerveld

en,

Naam: ……..

Komen als volgt overeen:

Artikel 1.
Het college van burgemeester en wethouders stemt erin toe dat u voor de uitvoering van uw taken persoonsgegevens, waarvoor de gemeente Westerveld verwerkingsverantwoordelijke of verwerker is, verwerkt, tenzij enige wettelijke bepaling aan het inzien van deze persoonsgegevens in de weg staat.

Artikel 2
Het is niet toegestaan om persoonsgegevens die u verwerkt met anderen, zowel binnen als buiten de gemeentelijke organisatie te delen, tenzij het delen een noodzakelijk uitvloeisel is van de opgedragen taken. Bij het delen van persoonsgegevens worden de wettelijke plichten en de richtlijnen van de gemeente Westerveld in acht genomen.

Artikel 3
Na afronding van uw taken bij de gemeente Westerveld blijft de geheimhoudingsverklaring van kracht.

Aldus opgemaakt in tweevoud op …….. te Westerveld.

Burgemeester en wethouders,
namens deze,

……. …….

Bijlage 2	Protocol gegevensverstrekking verwerkingsverantwoordelijke - gemeente Westerveld

Voor de uitvoering van taken kan de gemeente Westerveld voor verwerking van persoonsgegevens samenwerking aan gaan met andere verwerkingsverantwoordelijken. Binnen de samenwerkingsrelatie blijven alle betrokken verwerkingsverantwoordelijken zelfstandig verantwoordelijk voor de 'eigen' verwerkingen.

Dit protocol voorziet in de verstrekking van persoonsgegevens door de gemeente Westerveld aan de samenwerkingsrelatie om een gezamenlijk doel te bereiken voor zover deze persoonsgegevens noodzakelijk zijn voor de uitvoering van de taken van de desbetreffende samenwerkingsverband. Met inachtneming van het bij of krachtens de Algemene Verordening Gegevensbescherming (AVG) bepaalde geschiedt het verstrekken van persoonsgegevens overeenkomstig dit protocol.

Dit protocol gegevensverstrekking wordt voorafgaande aan elke eerste verstrekking voor een bepaald doel aan de partners in het samenwerkingsverband gezonden.

Protocol

1. In gevallen waarin de samenwerkingspartner(s) persoonsgegevens willen ontvangen van de gemeente Westerveld ter uitoefening van hun taken in de samenwerkingsafspraken, dien(t)en zij een daartoe strekkend verzoek in bij de gemeente Westerveld. In het verzoek worden de volgende onderwerpen beschreven:
- Doel en grondslag van de verwerking,
- Aantonen of contractspartij verwerkingsverantwoordelijke is,
- Indien contractspartij geen verwerkingsverantwoordelijke is dient het aan te tonen verwerker te zijn,
- Welke persoonsgegevens men van de gemeente wenst te ontvangen,
- Welke passende technische en organisatorische maatregelen de contractspartij heeft genomen om persoonsgegevens te verwerken,
- Welke maatregelen zijn genomen om verdere onrechtmatige verwerking te voorkomen,

2. Voor de uitvoering van wettelijke taken door de samenwerkingspartner kan de gemeente Westerveld alle bij haar bekende persoonsgegevens in een concrete situatie of in een verzameling concrete situaties ter verwerking overdragen aan de ander onder de restrictie dat enkel die persoonsgegevens worden overgedragen waarbij de samenwerkingspartner een aanwijsbaar belang heeft ten behoeve van de uitvoering van diens wettelijke taken.

3. Indien door de contractspartner geen wettelijke taak wordt uitgevoerd kan de gemeente Westerveld alle bij haar bekende persoonsgegevens in een concrete situatie ter verwerking overdragen aan de samenwerkingspartner, indien noodzakelijk ter bescherming van een vitaal belang van de betrokkene of diens naasten onder de restrictie dat enkel die persoonsgegevens worden overgedragen waarbij de samenwerkingspartner een aanwijsbaar belang heeft ten behoeve van de uitvoering van diens werkzaamheden. Indien de wettelijke grondslag en het vitaal belang ontbreken is overdracht van persoonsgegevens enkel mogelijk met uitdrukkelijke toestemming van de betrokkene.

4. De persoonsgegevens die op grond van artikel 2 en 3 van de gemeente Westerveld worden ontvangen zullen door de contractspartners worden verwerkt met inachtneming van de wettelijke voorschriften, waaronder de AVG, in welk kader de samenwerkingspartners voorafgaand aan de eerste verstrekking een privacy beleid zullen opstellen dat in overeenstemming is met dit protocol. Een exemplaar van dit beleidsplan zal aan de Gemeente Westerveld ter hand worden gesteld.

5. Voor de uitvoering van de verwerking door de contractspartners die geen verwerkingsverantwoordelijke zijn zal tussen gemeente Westerveld en de contractspartner een overeenkomst als bedoeld in artikel 28 lid 3 AVG worden opgesteld.

6. Contractspartners zullen de gemeente Westerveld onmiddellijk op de hoogte stellen van een datalek als bedoeld in artikel 33 AVG, alle noodzakelijke maatregelen nemen om het lekken te doen stoppen en om alle informatie en medewerking te verlenen waar de gemeente Westerveld om verzoekt.

7. Samenwerkingspartners zullen de van de gemeente Westerveld verkregen persoonsgegevens niet verder verwerken op een wijze die onverenigbaar is met de doeleinden waarvoor de persoonsgegevens zijn verkregen. Samenwerkingspartners zullen de persoonsgegevens niet openbaren of aan derden verstrekken, behoudens voor zover daartoe een wettelijke verplichting bestaat. Verdere verwerking van de

persoonsgegevens voor statistische of wetenschappelijk doeleinden wordt niet als onverenigbaar beschouwd, indien de nodige voorzieningen zijn getroffen ten einde te verzekeren dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden.

Bijlage 3 Overeenkomst verwerker - gemeente Westerveld ex artikel 28 lid 3 AVG

De gemeente Westerveld, gevestigd te Westerveld, verder te noemen de Verantwoordelijke,
ten deze rechtsgeldig vertegenwoordigd door …….

en

(naam bedrijf) gevestigd te (vestigingsplaats), verder te noemen de Verwerker,
ten deze rechtsgeldig vertegenwoordigd door (geslacht + naam)

verklaren te zijn overeengekomen, een overeenkomst als bedoeld in artikel 28, derde lid, van de AVG, tussen de gemeente Westerveld, nader te noemen de Verwerkingsverantwoordelijke, en (…), nader te noemen de Verwerker.

Definities
Artikel 1.
1.1 Begrippen met een hoofdletter hebben de betekenis als bedoeld in de Algemene Verordening Gegevensbescherming (AVG), tenzij uitdrukkelijk anders bepaald.

Ingangsdatum, duur en beëindiging
Artikel 2.
2.1 Deze overeenkomst gaat in op het moment van ondertekening en duurt voort zolang de in artikel 3.1 bedoelde overeenkomst voortduurt. Er bestaat samenhang tussen de in artikel 3.1 bedoelde overeenkomst en de onderhavige overeenkomst.
2.2 De gronden voor ontbinding en opzegging zijn gelijk aan de gronden van de in artikel 3.1 bedoelde overeenkomst.
2.3 Bij beëindiging, ontbinding of opzegging van deze overeenkomst, op welke grond of wijze dan ook, zal de Verwerker op eigen kosten en uit eigen beweging:
a. aan de Verantwoordelijke alle Persoonsgegevens ter beschikking stellen op de wijze en in het format dat de Verantwoordelijke wenst;
b. per direct de Verwerking van de Persoonsgegevens staken;
c. alle documenten waarin de Persoonsgegevens zijn vastgelegd aan de Verantwoordelijke ter beschikking stellen, en;
d. alle gegevens welke Verwerker van Verantwoordelijke heeft ontvangen verwijderen. Voor zover permanente verwijdering van Persoonsgegevens van de gegevensdrager niet mogelijk is, de gegevensdrager vernietigen.
2.4 Verwerker zal zodra de in het vorige lid beschreven werkzaamheden zijn voltooid, dit schriftelijk aan de Verantwoordelijke bevestigen.

Onderwerp van deze overeenkomst
Artikel 3.
3.1 Verwerker Verwerkt Persoonsgegevens in opdracht van de Verantwoordelijke in het kader van de uitvoering van <contract/nummer).
3.2 Verwerker Verwerkt Persoonsgegevens namens Verantwoordelijke ter uitvoering (……)
3.3 Verantwoordelijke kan, behoudens door de wettelijke vertegenwoordigers, in het kader van deze overeenkomst ook worden vertegenwoordigd door de contactpersoon. Contactpersoon namens de Verantwoordelijke is (contactpersoon invoegen), dan wel diens vervanger.

Naleving wet- en regelgeving
Artikel 4.
4.1 Verwerker Verwerkt gegevens ten behoeve van de Verantwoordelijke, in overeenstemming met diens instructies.
4.2 Verwerker heeft geen zeggenschap over de ter beschikking gestelde Persoonsgegevens. De Verwerker is niet gerechtigd de persoonsgegevens voor andere doeleinden te verwerken, dan de uitvoering van de in artikel 3.1 bedoelde overeenkomst.
4.3 Verwerker zal bij de Verwerking van Persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden, handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de bescherming van Persoonsgegevens. De Verwerker verwerkt Persoonsgegevens slechts in opdracht van de Verantwoordelijke en zal alle redelijke instructies van de Verantwoordelijke dienaangaande opvolgen, behoudens afwijkende wettelijke verplichtingen.
4.4 Verwerker zal te allen tijde op eerste verzoek van de Verantwoordelijke onmiddellijk alle Persoonsgegevens met betrekking tot deze bewerkersovereenkomst ter hand stellen.
4.5 Verwerker stelt de Verantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van betrokkenen,

zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet.
4.6 Verwerker zal de Verwerking van Persoonsgegevens louter binnen de grenzen van de Europese Economische Ruimte (“EER”) (doen) uitvoeren.

Geheimhoudingsplicht
Artikel 5.
5.1 Personen in dienst van, dan wel werkzaam ten behoeve van de Verwerker, evenals de Verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de Persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht of zijn taak daartoe noodzaakt. De medewerkers van de Verwerker tekenen hiertoe een geheimhoudingsverklaring. Verwerker staat er voor in dat alle personen die handelen onder zijn gezag en toegang hebben tot de Persoonsgegevens voornoemde geheimhouding in acht zullen nemen.
5.2 Indien de Verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de Verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de Verwerker de Verantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren en de Verantwoordelijke gelegenheid bieden zich tegen deze verstrekking te verzetten, tenzij wettelijke bepalingen dit verbieden.

Beveiligingsmaatregelen
Artikel 6.
6.1 Verwerker zal de verwerkingsverantwoordelijke zo spoedig mogelijk -doch uiterlijk binnen 24 uur na eerste ontdekking- informeren over alle (vermoedelijke) inbreuken op de beveiliging alsmede andere incidenten die op grond van wetgeving moeten worden gemeld aan de toezichthouder of betrokkene, onverminderd de verplichting de gevolgen van dergelijke inbreuken ongedaan te maken dan wel te beperken, al dan niet onder verbeurte van een boete in geval van niet nakoming van deze overeenkomst. Verwerker zal voorts, op het eerste verzoek van de verwerkingsverantwoordelijke, alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen..
6.2 Verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken en zal de verwerkingsverantwoordelijke op de hoogte stellen van materiële wijzigingen in het plan van aanpak
6.3 Verwerker zal het doen van meldingen aan de toezichthouder overlaten aan de verwerkingsverantwoordelijke.
6.4 Verwerker zal alle noodzakelijke medewerking verlenen aan het zo nodig, op het kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder en/of betrokkenen.
6.5 Verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen en geeft daar op eerste verzoek van de verwerkingsverantwoordelijke inzicht in.

Controle naleving en rapportages
Artikel 7:
7.1 Verwerker neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt ten dienste van de verwerkingsverantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking.
7.2 Verwerkingsverantwoordelijke is te allen tijde gerechtigd de nakoming van de verplichtingen uit onderhavige overeenkomst door Verwerker te (doen) controleren. Verwerker zal aan een dergelijke controle alle noodzakelijke medewerking verlenen.
7.2. Verantwoordelijke zal de audit slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan de Verwerker.
7.4 Verwerker verbindt zich om binnen de door de verwerkingsverantwoordelijke te bepalen termijn, of door verwerkingsverantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie.. Hierdoor kan de verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, zich een oordeel vormen omtrent naleving van deze overeenkomst.. Verantwoordelijke, of de door de Verantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen, zulks onverminderd het recht van verantwoordelijke de informatie die betrekking heeft op de naleving van de onderhavige overeenkomst (al dan niet in rechte) jegens Betrokkene te gebruiken.
7.5 Verwerker staat er voor in, de door de verwerkingsverantwoordelijke of ingeschakelde derde, aangegeven aanbevelingen ter verbetering binnen de daartoe door de verwerkingsverantwoordelijke te bepalen redelijke termijn uit te voeren.
7.6 Verwerker rapporteert jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze overeenkomst.
7.7 Naast rapportages door verwerker en controles door verwerkingsverantwoordelijke of controlerende instantie in opdracht van de verwerkingsverantwoordelijke, kunnen beide partijen ook overeenkomen gebruik te maken van een third party memorandum opgesteld door een onafhankelijke externe deskundige.

7.8 De redelijke kosten van de controle worden gedragen door de partij die de kosten maakt, tenzij uit de controle blijkt dat de verwerker enig punt uit de verwerkersovereenkomst niet heeft nageleefd. In dat geval worden de kosten van de controle gedragen door de verwerker.

Inschakeling derden
Artikel 8.
8.1 Verwerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande schriftelijke toestemming van de Verantwoordelijke. De Verantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze overeenkomst.
8.2 Verwerker staat er voor in dat eventueel door haar ingeschakelde derden de in deze bewerkersovereenkomst gestelde voorwaarden onverkort zullen naleven en dat deze derden zich eveneens zullen richten naar instructies van de Verantwoordelijke.
8.3 Verwerker blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze bewerkersovereenkomst.

Wijziging overeenkomst
Artikel 9.
9.1 Wijziging van deze overeenkomst kan slechts schriftelijk plaatsvinden middels een door beide partijen geaccordeerd voorstel.
9.2 Indien een wijziging in de verwerkte persoonsgegevens of een wijziging in de betrouwbaarheidseisen Verantwoordelijke aanleiding geeft (de voorwaarden van) deze overeenkomst te wijzigen en Verwerker niet bereid is op redelijke voorwaarden met die wijziging in te stemmen c.q. te kennen geeft deze (gewijzigde) diensten niet te kunnen verrichten, dan is Verantwoordelijke gerechtigd deze overeenkomst en de in artikel 3.1 bedoelde overeenkomst met onmiddellijke ingang op te zeggen.

Aansprakelijkheid
Artikel 10
10.1 Indien de Verwerker tekortschiet in de nakoming van de verplichting uit deze overeenkomst kan Verantwoordelijke hem in gebreke stellen. Verwerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de Verwerker een redelijke termijn wordt gegund om alsnog haar verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is Verwerker in verzuim.
10.2 Verwerker is aansprakelijk voor alle schade of nadeel voortvloeiende uit het niet-nakomen van, of in strijd handelen met de bij of krachtens de AVG gegeven voorschriften en/of het niet-nakomen van, of in strijd handelen met het in deze overeenkomst bepaalde, mits de schade is ontstaan is door toedoen of nalaten van Verwerker.
10.3 De eventueel in de in artikel 3.1 bedoelde overeenkomst opgenomen beperking van aansprakelijkheid is niet van toepassing op schade die voortvloeit uit het niet of onvoldoende naleven van de onderhavige bewerkersovereenkomst.
10.4 Verwerker vrijwaart Verantwoordelijke voor alle kosten die verband houden met handhaving door de toezichthouder(s) en eventuele door de toezichthouder(s) aan Verantwoordelijke opgelegde boetes, voor zover die kosten en boetes verband houden met doen of nalaten van Verwerker dat op grond van deze overeenkomst aan Verwerker is toe te rekenen.

Rangorde
Artikel 11
Voor zover enige bepaling van deze overeenkomst in strijd is met hetgeen in de in artikel 3 bedoelde overeenkomst(en) is bepaald, prevaleert hetgeen in de onderhavige overeenkomst is bepaald.

Citeertitel
Artikel 12.
Deze overeenkomst kan worden aangehaald als „Verwerkersovereenkomst uitvoering <.....>"

Aldus in tweevoud opgesteld en getekend de dato
Namens de Verantwoordelijke van de gemeente Westerveld

Namens de <nader in te vullen gegevens Verwerker><nader in te vullen gegevens vertegenwoordiger Verwerker, zoals genoemd in de aanhef>

Bijlage 4 Naam verwerking

Naam verwerking :

Verwerkingsverantwoordelijke :

Team :
Eigenaar :
Contactpersoon :
Relaties met andere verwerkingen :

Verwerker :
Contactpersoon verwerker :
FG :
Verwerkersovereenkomst :

Datum :
Versie :

Verloop van het proces

Doel van de verwerking
Grondslag van de verwerking
Wet/Taak/Taak accent
Bewaartermijn

Categorieën betrokkenen

Interne en externe ontvangers (data gebruikers) en reden waarom

Persoonsgegevens en kenmerken				
Persoonsgegeven	Bijzonder j/n	Bron data	Opslagplek	Bewaartermijn

Naam opslagplek	Beveiligingsmaatregelen

Wijze communicatie aan betrokkene over verwerking

Wijze waarop persoonsgegevens na bereiken doel worden gewist / gearchiveerd