Gemeente Súdwest-Fryslân

GEMEENTEBLAD

Officiële uitgave van de gemeente Súdwest-Fryslân

Nr. 251049

8 juni

2023

Privacybeleid Sociaal Domein gemeente Súdwest-Fryslân

Het college van burgemeester en wethouders van de gemeente Súdwest-Fryslân;

Heeft overwogen dat:
- het van belang is voor de verwerking van persoonsgegevens in het kader van de gemeentelijke taken binnen het Sociaal Domein, beleid vast te stellen;
- het wenselijk is dit beleid te publiceren en daarmee uitvoering te geven aan artikel 6 van de Bekendmakingswet;

besluit:

vast te stellen het Privacybeleid Sociaal Domein gemeente Súdwest-Fryslân.

Inhoudsopgave

Inleiding

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming in werking getreden. De gemeente Súdwest-Fryslân heeft in dat kader in april 2018 privacy beleid opgesteld voor de hele gemeente op welke wijze er wordt omgegaan met de persoonsgegevens van de burger. Het sociale domein vraagt om een verdere en specifieke uitwerking.

Het sociaal domein omvat de gemeentelijke taken op het gebied van werk, participatie, zorg, zelfredzaamheid en jeugdhulp. De uitvoering hiervan gebeurt op basis van de Wmo 2015, de Participatiewet, de Jeugdwet, Wet gemeentelijke schuldhulpverlening, maar ook vallen diverse wetten zoals IOAZ, IOAW en diverse gemeentelijke regelingen zoals de gehandicaptenparkeerkaart hier onder. Aanverwante taken zoals handhaving bij leerplicht, leerlingenvervoer, het voorkomen van vroegtijdig schoolverlaten (RMC, regionale Meld en Coördinatiefunctie) en taken voortkomend uit de Wet publieke gezondheid (GGD en jeugdgezondheidszorg) vallen hier niet onder.

Met het decentraliseren van taken binnen het sociaal domein vanuit de landelijke overheid naar de gemeenten, hebben gemeenten meer verantwoordelijkheden gekregen, worden er meer persoonsgegevens verwerkt en is de noodzaak voor integraal werken, ook op het gebied van privacy, groter geworden. Een integrale dienstverlening aan de inwoner is daarbij het uitgangspunt. Hieronder verstaan we dat er samenhang is in de aanpak. Enerzijds door aandacht te hebben voor meerdere leefgebieden en vraagstukken van de inwoner en anderzijds door als professionals met elkaar samen te werken, processen, werkwijze en expertise op elkaar af te stemmen en tot een gezamenlijke aanpak voor de hulpvraag van de inwoner te komen. Dit is in het beleidsdocument van de gemeente “Veerkracht in het Sociaal Domein” uiteengezet. Bondig samengevat in: één gezin, één plan, één aanpak.

Om integrale dienstverlening te kunnen bieden is het kunnen delen van bepaalde gegevens binnen de verschillende domeinen een randvoorwaarde. Inwoners moeten er echter wel op kunnen vertrouwen dat de professionals zorgvuldig omgaan met persoonsgegevens, dat hun privacy optimaal wordt ge-

waarborgd en dat dit binnen de kaders van de wet gebeurt. Een efficiënte en integrale dienstverlening moet in balans zijn met de privacy en keuzevrijheid voor inwoners. Het uitwisselen en benutten van informatie over inwoners is een middel en geen doel. Het middel staat ten dienste van de dienstverlening aan die inwoner zelf. Het is daarom van groot belang dat het gebruik van die informatie zorgvuldig gebeurt en de privacybelangen van de inwoner continu gewaarborgd zijn. Hierbij past het dat we terughoudend zijn met het vastleggen en uitwisselen van persoonsgegevens. In de verschillende wetten en regelingen binnen het Sociaal Domein is geen ruimte voor een integrale aanpak opgenomen. Wel is er een wetsvoorstel: Wet Aanpak meervoudige problematiek sociaal domein (Wams) ontwikkeld dat wel meer ruimte geeft voor een integrale aanpak en het uitwisselen van persoonsgegevens binnen de verschillende onderdelen in het sociale domein. Op dit moment ligt het wetsvoorstel ter advisering bij de Raad van State.

Om te voldoen aan de huidige wetgeving en beleid, én aan de overkoepelende privacywetgeving van De Algemene Verordening Gegevensbescherming (AVG) is er een privacybeleid sociaal domein voor de gemeente Súdwest-Fryslân opgesteld.
Dit privacybeleid:

- Biedt richtlijnen voor de verwerking van persoonsgegevens in verband met de ondersteuning van inwoners;
- Draagt bij aan een goede uitvoering van gemeentelijke werkzaamheden in het sociaal domein van Súdwest-Fryslân;
- Is van toepassing op alle medewerkers die werken voor of namens het sociaal domein, zoals beschreven en afgebakend in dit hoofdstuk, van de Gemeente Súdwest-Fryslân;
- Biedt helderheid over de positie en de rol van de gemeente Súdwest-Fryslân waar het gaat om verwerking van persoonsgegevens;
- Draagt bij aan het vertrouwen van de betrokken inwoners. Onze inwoners moeten ervan op aan kunnen dat zorgvuldig met hun belangen en gegevens wordt omgegaan;
- Heeft betrekking op elke verwerking van persoonsgegevens binnen het sociaal domein van de gemeente Súdwest-Fryslân en elke vorm (mondeling, schriftelijk, elektronisch etc.);
- Is voor zover mogelijk ook van toepassing op de uitvoering van de individuele voorzieningen voor inwoners door (zorg)aanbieders van bijvoorbeeld huishoudelijke hulp, begeleiding, jeugdhulp etc. Deze verantwoordelijkheden in de samenwerking moeten worden vastgelegd in bv een verwerkersovereenkomst.

1. Definities

1.1 Algemene Verordening Gegevensbescherming (AVG):
De AVG regelt per 25 mei 2018 de verwerking van persoonsgegevens in de hele Europese Unie. Deze verordening vervangt de Wet bescherming persoonsgegevens en biedt handvatten aan de hand waarvan persoonsgegevens verwerkt, gedocumenteerd en beschermd dienen te worden, zowel digitaal als op schrift.

1.2 Betrokkene / Cliënt:
Een persoon op wie de ondersteuning vanuit het sociaal domein van de gemeente is gericht.

1.3 Bijzondere persoonsgegevens:
Gegevens die iets zeggen over iemands godsdienst of levensovertuiging, ras, etnische afkomst, politieke gezindheid, gezondheid, genetische gegevens, seksuele leven en lidmaatschap van een vakvereniging of strafrechtelijke veroordelingen en feiten.

1.4 Cliëntsysteem:
De persoon of personen met wie de betreffende inwoner in gezinsverband leeft of heeft geleefd en op wie de ondersteuning vanuit het sociaal domein gericht is, of die op enigerlei wijze is of zijn betrokken bij de ondersteuning aan de cliënt.

1.5 Derde(n):
Iedere persoon of instelling, niet zijnde de cliënt, een lid van het cliëntsysteem of een medewerker die namens de gemeente een taak binnen het sociaal domein van de gemeente uitvoert.

1.6 Dossier:
Een systematische gebundelde verzameling van (persoons)gegevens rondom de ondersteuning vaneen cliënt(systeem).

1.7 Hulp-/dienstverlener:

Een persoon die hulp- en dienstverleningstaken verricht vanuit het sociaal domein van de gemeente ten behoeve van cliënten. Het gaat hierbij zowel om personen werkzaam in de toegang tot de voorzieningen als in de uitvoering van de overige voorzieningen zoals jeugdhulp, Wmo (bv.consulenten en klantmanagers) en de Participatiewet (levensonderhoud, bijz. bijstand, (gemeentelijke) minimaregelingen, etc.).Dit betreft ook vrijwilligers of stagiaires die onder verantwoordelijkheid van de gemeente deze taken uitvoeren. Deze personen zijn belast met de verwerking van cliëntgegevens in het kader van de uitoefening van hun functie.

1.8 Inwoner:
Alle personen ingeschreven en woonachtig binnen de gemeente.

1.9 Medewerker ondersteunende diensten:
Een persoon die namens de gemeente binnen het sociaal domein taken verricht die ondersteunend zijn aan de hulp-/dienstverlener, zoals administratieve, financiële of andere ondersteuning (bv. applicatiebeheerders, kwaliteitsmedewerkers, medewerkers bezwaar- en beroep, beleidsmedewerkers, medewerkers uitkeringsadministratie, medewerkers administratieve ondersteuning en archivering).

1.10 Ondersteuning:
Alle handelingen en activiteiten die namens en onder verantwoordelijkheid van de gemeente worden verricht binnen het sociaal domein en die direct betrekking hebben op de dienstverlening aan cliënt(systeem).

1.11 Persoonsgegevens:
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene/cliënt"). Als identificeerbaar wordt beschouwd een natuurlijk 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.

1.12 Privacy:
Privacy heeft betrekking op het eerbiedigen van de persoonlijke levenssfeer en omvat de bescherming van persoonsgegevens, vertrouwelijke communicatie en integriteit van persoon en lichaam. Het is een mensenrecht en een fundamentele vrijheid.

1.13 Transparantiebeginsel:
Transparantie is in de AVG opgenomen als een apart beginsel. Het dient transparant te zijn voor een natuurlijk persoon dat zijn persoonsgegevens worden verwerkt en in hoeverre dit gebeurt. Het transparantiebeginsel verplicht de verwerkingsverantwoordelijke om te communiceren in een beknopte en transparante, begrijpelijke en gemakkelijk toegankelijke vorm. Daarnaast moet deze informatie in duidelijke en eenvoudige taal worden opgesteld. Deze informatie en communicatie moet schriftelijk of met andere middelen (bv. elektronisch) verstrekt worden.

1.14 Verwerkingsverantwoordelijke:
Natuurlijk persoon, rechtspersoon, bestuursorgaan of ieder ander die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt en hierbij toeziet op naleving van de privacywetgeving. Binnen het sociaal domein geldt dat onder deze definitie valt de eindverantwoordelijke zoals opgenomen in het hoofdstuk governance.

1.15 Verwerker:
Degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid, zonder aan zijn rechtstreeks gezag te zijn onderworpen. Binnen het sociaal domein van de gemeente betreft dit een ieder die persoonsgegevens verwerkt, in dienst van de gemeente.

1.16 Verwerking van persoonsgegevens:
Het verwerken van persoonsgegevens betreft elke handeling met betrekking tot die gegevens. Hierbij kan worden gedacht aan verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, samenbrengen en afschermen.

1.17 Wettelijke vertegenwoordiger:
De persoon die het gezag over een minderjarige of wilsonbekwame uitoefent.

2. Visie en uitgangspunten

In het document "Veerkracht in het sociaal domein" zijn de visie en de uitgangspunten met betrekking tot privacy in het sociaal domein van de gemeente vastgelegd. Deze vormen mede de basis voor het privacy beleid.

Visie op privacy in het sociaal domein:
We streven ernaar alle gegevens van inwoners op een juiste manier te verwerken. De inwoner moet hier op kunnen vertrouwen. We respecteren en beschermen de persoonsgegevens van de inwoners en denken en handelen in lijn met het recht op bescherming van de persoonlijke levenssfeer. Alle medewerkers binnen het sociaal domein van de gemeente Súdwest-Fryslân hebben de verantwoordelijkheid om zorgvuldig en bewust om te gaan met zowel de eigen persoonsgegevens als die van een ander. De medewerkers worden op een gezagvolle wijze aangezet tot het nemen van verantwoordelijkheid en maatregelen met betrekking tot gegevensverwerking.

We erkennen de noodzaak van inzameling en verwerking van persoonsgegevens voor de ondersteuning aan inwoners. Er wordt bij besluitvorming een afweging gemaakt tussen het fundamentele recht op privacy en de gemeentelijke opgaven in het sociaal domein.

We zijn ons ervan bewust dat aan iedere gegevensverwerking risico's verbonden zijn op het vlak van privacybescherming. We hebben aandacht voor het feit dat de inzet van technologieën voor de verwerking van persoonsgegevens een zeer belangrijke factor is voor de verhoging van het welzijn en de welvaart van de inwoners.

Gezamenlijke uitgangspunten met betrekking tot privacy in het sociaal domein;
- De hulpvraag/aanvraag van de inwoner is leidend. Ook als het gaat om verwerken of delen van persoonsgegevens is de hulpvraag/aanvraag van de inwoner leidend. De informatie die verwerkt of gedeeld wordt is dus altijd gerelateerd aan die hulpvraag.
- De inwoner wordt altijd geïnformeerd over wat er met zijn of haar gegevens gebeurt en waarom. Dit kan zowel mondeling als schriftelijk, waarbij wordt uitgegaan van het transparantiebeginsel.
- De gemeente Súdwest-Fryslân wil door dichtbij de inwoners te staan en in samenwerking met ketenpartners problemen of vragen vroegtijdig signaleren. Het vroegtijdig vastleggen van deze signalen of uitwisselen ervan met ketenpartners is een aspect wat de privacy raakt.
- Medewerkers maken per casus/aanvraag een afweging over de doelbinding, proportionaliteit en subsidiariteit als het gaat om het verwerken of delen van persoonsgegevens van de inwoner.
- De benodigde gegevensverwerking ten behoeve van de vraagverheldering en het opstellen van een plan van aanpak wordt in principe samen met de inwoner bepaald en uitgevoerd. Zo heeft het de voorkeur dat de betrokken inwoner aanwezig is bij het overleg over zijn/haar plan van aanpak.
- Alleen de betrokken medewerkers, die vanuit hun wettelijke taak met de (aan)vraag van de burger bezig zijn, hebben toegang tot het volledige dossier in de daarvoor bestemde applicatie.

Voor de medewerkers in het gebiedsteam is er nog een extra uitgangspunt namelijk:
- Binnen de gebiedsteams van de gemeente Súdwest-Fryslân wordt gewerkt met een brede vraagverheldering en wordt er een bredere uitvraag gedaan dan de oorspronkelijke hulpvraag.

<u>Wat houdt de brede vraagverheldering in waar het gebiedsteam mee werkt?</u>
In de gemeente Súdwest-Fryslân willen we naar de mens als geheel kijken, met wat er niet goed gaat maar juist ook wat er wel goed gaat. Naar de hele mens in zijn of haar omgeving. Zorgen of problemen staan niet op zichzelf en hebben invloed op andere gebieden. Zo is bekend dat financiële problemen zorgen voor stress in de relatie of de opvoeding. Aan de andere kant kan iets dat heel goed gaat, bijvoorbeeld goede contacten met familie of in de buurt, een tegenwicht bieden aan dat wat niet vanzelf gaat.
Soms is het zelfs zo dat een verbetering op een heel ander gebied ervoor zorgt dat het probleem minder of anders wordt. Om die reden vraagt de gebiedsteamwerker naar de reden van de aanmelding én naar andere zaken die in ieders leven spelen, zoals gezondheid, hoe gaat het met de kinderen, eenzaamheid, de woonsituatie en het netwerk. De inwoner kan zelf aangeven of hij/zij hierover in gesprek wil. Wil de bewoner het enkel hebben over de eerste aanvraag/hulpvraag dan worden die gegevens verwerkt. Met toestemming en in samenspraak met de inwoner kan er vorm gegeven worden aan de brede vraagverheldering en dus ook gegevens betreffende andere levensdomeinen worden verwerkt. Dit in het kader van het algemene belang en het welzijn van de inwoner. Het gesprek begint met een uitleg aan de inwoner waarom de werkwijze wordt gehanteerd. Indien de inwoner aangeeft, niet mee te willen werken aan de brede vraagverheldering, zal deze niet plaatsvinden en worden er alleen de benodigde gegevens

verwerkt die behoren bij de oorspronkelijke hulpvraag. Op deze wijze wordt de privacy van de inwoner voldoende beschermt en bepaalt de inwoner zelf welke gegevens er verwerkt worden.

Deze werkwijze, uit het oogpunt van het welzijn van de inwoner, gebeurt in het kader van het algemeen belang dat de gemeente heeft op grond van de uitvoering van de wetten in het Sociaal Domein. Dit is tevens één van de grondslagen in het kader van de AVG.

3. Wettelijk kader

Het recht op eerbiediging van de persoonlijke levenssfeer vindt zijn grondslag in verschillende verdragen en in de Grondwet. Verwerking kan alleen als hiervoor een wettelijke grondslag is (zie bijlage II). De verwerking moet beperkt blijven tot wat voor het te bereiken doel noodzakelijk is. Een belangrijk vraag die daarbij telkens moet worden beantwoord is: kan van elk van de uit te wisselen gegevens goed worden aangegeven waarom ze nodig zijn voor het bereiken van het doel?

Internationale verdragen
De betekenis van het recht op eerbiediging van de persoonlijke levenssfeer is verstrekkend, met name door de brede interpretatie die het Europees Hof voor de rechten van de mens (EHRM) daaraan geeft. Artikel 8 EVRM bepaalt dat iedereen recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Hierbij is duidelijk dat inmenging in de persoonlijke levenssfeer, zoals de verwerking van persoonsgegevens, alleen is toegestaan als het noodzakelijk is en een gerechtvaardigde grondslag heeft.

Europese Algemene Verordening Gegevensverwerking (AVG)
De Europese AVG vervangt de Wet bescherming persoonsgegevens en heeft een rechtstreekse werking in Nederland. In de AVG is het recht op privacy verder uitgewerkt. Naast de AVG kunnen ook in specifieke wetten bepalingen staan over het verwerken van persoonsgegevens.
In de AVG is uitvoerig opgenomen wat wordt verstaan onder persoonsgegevens en het verwerken van persoonsgegevens. Persoonsgegevens kunnen worden verwerkt door een verwerkingsverantwoordelijke of door een verwerker. Een gezamenlijke verantwoordelijkheid is eveneens mogelijk. De AVG eist dat persoonsgegevens op een behoorlijke en zorgvuldige manier worden verwerkt en alleen voor duidelijk omschreven doelen worden gebruikt. In de AVG zijn grondslagen opgenomen die voor informatie-uitwisseling in het sociale domein kunnen bestaan. De AVG bevat een aantal andere zeer relevante normen. Een voorbeeld is de plicht om passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Dit is de beveiligingsplicht. Deze plicht rust bij de gemeenten als verwerkingsverantwoordelijke en strekt zich uit tot verwerkingen die elders worden uitgevoerd.

Nederlandse wetten
Naast de hierboven beschreven regelgeving zijn er meerdere bijzondere Nederlandse wetten in het sociaal domein: de Jeugdwet, de Wmo 2015, de Participatiewet en de Wet gemeentelijke schuldhulpverlening (Wgs), maar ook wetten zoals de IOAZ en de IOAW en aanvullende gemeentelijke regelingen zoals de beleidsregels gehandicaptenparkeerkaarten en gehandicaptenparkeerplaatsen 2020 gemeente Súdwest-Fryslân. Deze wetten en regelingen geven meer in detail de juridische grondslagen voor de uitwisseling van persoonsgegevens in en tussen sectoren. Daarnaast heeft het sociaal domein uiteraard ook te maken met meer generieke wet- of regelgeving. De Algemene Wet Bestuursrecht is daar een voorbeeld van.

4. Algemene beleidsbepalingen

In dit hoofdstuk zijn de bepalingen met betrekking tot privacy beschreven die belangrijk zijn om zowel aan onze visie en uitgangspunten binnen het sociaal domein als aan het wettelijk kader te kunnen voldoen. Ook is waar mogelijk beschreven hoe we in onze gemeente uitvoering geven hieraan. Door de brede vraagverheldering binnen de gebiedsteams worden er meer persoonsgegevens verzameld dan voor de eerste hulpvraag noodzakelijk is. We houden steeds voor ogen dat het welzijn van de inwoner centraal staat en het verwerken van persoonsgegevens gebeurt daarom met respect voor de rechten van de inwoner. De informatie die verwerkt of gedeeld wordt, is dus altijd gerelateerd aan die hulpvraag/aanvraag of de uitgebreidere hulpvraag in het kader van de brede vraagverheldering, in ieder geval met toestemming. In dit hoofdstuk is ook aandacht voor de communicatie aan de inwoner. De inwoner moet geïnformeerd worden over wat er met zijn of haar gegevens gebeurt, waarom dat gebeurt en daarvoor ook toestemming moet geven, indien dit niet bij wet geregeld is.

4.1 Doelbinding en noodzaak

Binnen het sociaal domein van de gemeente worden alleen die gegevens verwerkt die noodzakelijk zijn voor een bepaald doel. Deze gegevens worden niet later hergebruikt (zonder toestemming hiervoor van de betrokkene). Iedere ondersteuningsvraag is een vraag op zich en dient opnieuw beoordeeld te worden. 'Need to know' is dus geen 'nice to know'. Bij iedere hulpvraag geldt een andere 'need to know'. Voor gegevensverwerking geldt in elke situatie de zogenaamde noodzakelijkheidstoets. Dit houdt in dat (persoons)gegevens alleen verwerkt mogen worden als dit noodzakelijk is voor een bepaald doel en dat alleen de voor dat doel noodzakelijke gegevens verwerkt worden. Dit heet ook wel de 'dubbele noodzaak', die gaat over zowel het feit 'dat' gegevens verwerkt worden als 'welke' gegevens verwerkt worden. Het noodzakelijkheidsvereiste betekent dat 'nuttig' of 'handig' onvoldoende reden is om persoonsgegevens te verwerken. Indien het een individuele aanvraag van een inwoner betreft voor een bepaalde voorziening, die rechtstreeks wordt aangevraagd bij de gemeente, is het duidelijker welke gegevens noodzakelijk zijn om te verwerken.

Vanuit een juridisch oogpunt wordt de noodzakelijkheidstoets ingevuld door de vereisten van proportionaliteit en subsidiariteit. Proportionaliteit betekent dat er niet meer privacy-inbreuk wordt gepleegd dan nodig. Het gaat daarbij over de verhouding tussen doel en middel: is de gegevensverwerking nodig om het doel te bereiken? Subsidiariteit betekent dat het middel dat het minst inbreuk maakt op de privacy om het doel te bereiken de voorkeur heeft. Het gaat dus over de vraag of er alternatieven zijn die minder privacygevoelig zijn of meer waarborgen bieden. Proportionaliteit en subsidiariteit hangen met elkaar samen.

Bij de brede vraagverheldering vanuit het gebiedsteam wordt er tevens uitvraag gedaan over gegevens die in eerste instantie niet tot de hulpvraag van de inwoner behoren. Door de inwoner eerst duidelijke uitleg te geven waarom wordt gewerkt met de brede vraagverheldering en ook alleen maar gegevens te verwerken indien er toestemming is verleend, draagt dit bij aan doelbinding en aan een integrale aanpak in het belang (dus noodzaak)voor de inwoner. De toestemming is dan ook de grondslag voor de verwerking.

4.2 Verwerkingsgrondslagen

De meest voor de hand liggende grondslagen voor gegevensverwerking op grond van de AVG in de context van het sociaal domein van de gemeente zijn:

- het nakomen van een wettelijke verplichting (waaraan de verwerkingsverantwoordelijke is onderworpen) (Artikel 6 lid 1 sub c AVG);
- de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de gemeente is opgedragen;

Deze verwerkingsgrondslagen (artikel 6 lid 1 sub e AVG) vinden hun basis in de Wmo 2015, de Jeugdwet, Participatiewet, de Wgs maar ook in diverse wetten zoals IOAZ, IOAW, en diverse gemeente regelingen zoals de beleidsregels gehandicaptenparkeerkaarten en gehandicaptenparkeerplaatsen 2020 gemeente Súdwest-Fryslân etc.
Gegevensverwerking is ook gerechtvaardigd als deze noodzakelijk is ter bestrijding van een ernstig gevaar voor de gezondheid van de betrokkene. Deze verwerkingsgrondslag 'vitaal belang' (Artikel 6 lid 1 sub d AVG) moet wel strikt worden geïnterpreteerd. Er moet een dringende noodzaak zijn om de gegevens van de betrokkene te verwerken. Het gaat hierbij om acute nood en komt zelden voor.
Gegevensverwerking is ook gerechtvaardigd als deze noodzakelijk is ter bestrijding van een ernstig gevaar voor de gezondheid van de betrokkene. Deze verwerkingsgrondslag 'vitaal belang' (Artikel 6 lid 1 sub d AVG) moet wel strikt worden geïnterpreteerd. Er moet een dringende noodzaak zijn om de gegevens van de betrokkene te verwerken. Het gaat hierbij om acute nood en komt zelden voor.

4.3 Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gegevens over iemands: ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, gegevens over gezondheid, seksueel gedrag of seksuele gerichtheid, genetische gegevens en biometrische gegevens.

Waar 'gewone' persoonsgegevens in principe mogen worden verwerkt, als dat op basis van een grondslag en zorgvuldig gebeurt, is de verwerking van 'bijzondere persoonsgegevens' juist verboden, behalve strenge wettelijke uitzonderingen. Bijzondere persoonsgegevens zijn zo gevoelig dat de verwerking ervan iemands privacy zeer kan beïnvloeden. In principe worden bijzondere persoonsgegevens dus niet verwerkt. Bijzondere persoonsgegevens worden wel verwerkt als dit strikt noodzakelijk is voor de ondersteuning aan de betrokkene, in het kader van vitale belangen en de uitoefening van sociale zekerheids- en sociale beschermingsrechten. De betrokkene moet dan wel hiervoor toestemming geven. Bovendien geldt onverkort het noodzakelijkheidsvereiste. Binnen het sociaal domein gaat het meestal over gegevens met betrekking tot de gezondheid en/of strafrechtelijke gegevens.
Denk hierbij bijvoorbeeld aan medische gegevens. Zo mogen er geen medische rapporten of diagnoses worden verwerkt. Wel mag er een omschrijving gegeven worden van de beperkingen om een goed

beeld te vormen van de ondersteuning die de inwoner nodig heeft. Door het gedrag en/of de beperking te omschrijven en niet de diagnose kan er gerichte hulp ingezet worden op de juiste ondersteuning en worden er geen bijzondere persoonsgegevens verwerkt.

4.4 Toestemming van betrokkene
Voordat gegevens worden verworven en verwerkt, wordt de inwoner nadrukkelijk om toestemming gevraagd (Artikel 6 lid 1 sub a AVG) bij voorkeur schriftelijk, tenzij de verwerking noodzakelijk is op grond van de wet. Voor een geldige toestemming moet aan een aantal randvoorwaarden worden voldaan. De toestemming moet onder andere:

- aangetoond kunnen worden door de verwerkingsverantwoordelijke (dus bij voorkeur schriftelijk);
- te allen tijde ingetrokken kunnen worden door de inwoner (de verwerking met toestemming blijft, alleen vanaf het moment van intrekken stopt de verwerking als hiervoor geen wettelijke grondslag is);
- het moet voor de inwoner duidelijk zijn welke gegevens worden verwerkt en waarom.

Ook is het belangrijk dat de toestemming wordt gevraagd vóórdat de persoonsgegevens worden verzameld en de inwoner vooraf is geïnformeerd over het gebruik van de gegevens. De toestemming moet ook vrijelijk gegeven kunnen worden door de inwoner. Niet onder druk van dat anders de hulpverlening niet uitgevoerd wordt bijvoorbeeld. Met name als er voor een specifiek onderdeel uitdrukkelijke toestemming (bijvoorbeeld: voor informatie delen met derden op basis van de Jeugdwet moet op basis van de wet toestemming zijn verleend) van de betrokkene nodig is, is het verkrijgen van de toestemming van groot belang. Dit is bijvoorbeeld zo bij het uitwisselen van persoonsgegevens met derden en bij het verbreken van de wettelijke geheimhoudingsplicht.

Toestemming kan zowel mondeling als schriftelijk worden gegeven (bij voorkeur schriftelijk). Diegene die de toestemming heeft gekregen van de inwoner, moet kunnen aantonen dat de toestemming is verleend. Bij een mondelinge toestemming kan dus een discussie ontstaan.
Een schriftelijke verklaring is ook mogelijk via elektronische middelen. Is er sprake van mondelinge toestemming, dan wordt dit opgenomen in het dossier. Er mag geen enkele twijfel bestaan over het feit dat toestemming is verleend en ook voor welke specifieke verwerking toestemming is gegeven. Daarnaast moet kunnen worden bewezen dat is voldaan aan de informatieplicht (artikel 12 AVG). Er moet dus altijd expliciet worden vastgelegd welke gegevens worden gedeeld, waarvoor, of betrokkene het daarmee eens is en welke informatie/persoonsgegevens zijn verstrekt.

Ook in de door de gemeente binnen het sociaal domein gebruikte systemen, ten behoeve van de integrale ketensamenwerking, kan alleen gewerkt worden binnen de kaders van de privacywetgeving en dus met toestemming van de betrokkene. Binnen deze systemen is het van belang dat de autorisaties goed geregeld zijn. Alleen de betrokken medewerkers mogen toegang hebben tot de gegevens van de inwoner.

4.5 Geheimhoudingsplicht
Op grond van de Ambtenarenwet wordt er verwacht dat iedere interne medewerker werkzaam binnen de gemeente, de eed of belofte aflegt en ondertekent zowel een integriteitsverklaringsverklaring als geheimhoudingsverklaring nieuwe medewerker. Deze hebben betrekking op iedere vorm van werkzaamheden die worden verricht binnen het sociaal domein. Voor externe medewerkers geldt dat zij een integriteit- en geheimhoudingsverklaring externe inhuur dienen te tekenen. Een getekende geheimhoudingsverklaring draagt bij aan het limiteren van de verwerking van persoonsgegevens. Het limiteren van persoonsgegevens mag het uitvoeren van de wettelijke taak niet in de weg te staan, om die reden kan doorbreking van de geheimhoudingsplicht nodig zijn.
Naast de grondslag die nodig is voor de verwerking van persoonsgegevens moet er voor het delen van persoonsgegevens aan derden en daarmee het doorbreken van de geheimhoudingsplicht, een aparte grondslag zijn. Zo'n grond kan zijn gelegen in een wettelijk voorschrift dat tot verstrekking van persoonsgegevens verplicht (bijvoorbeeld voor de financiële afwikkeling van declaraties, de verwijsindex risicojongeren (VIR), een melding bij Veilig Thuis, bepaalde verstrekkingen aan de Belastingdienst en bij gedwongen jeugdhulp). Of omdat er sprake is van een - zeer uitzonderlijke - situatie van een 'conflict van plichten.'

Toestemming van betrokkene kan ook een grond voor doorbreking van de geheimhoudingsplicht vormen. De betrokkene dient dus expliciete, gerichte toestemming te geven alvorens gegevens verstrekt mogen worden aan derden. Is alles in het werk gesteld om toestemming van de inwoner de verkrijgen, verkeert de hulp-/dienstverlener in gewetensnood door het handhaven van de geheimhouding, is er geen andere weg mogelijk dan het doorbreken van de geheimhoudingsplicht en is er sprake van ernstig gevaar voor de veiligheid en/of gezondheid als de geheimhouding niet wordt doorbroken, dan kunnen gegevens zonder toestemming worden gedeeld (het betreft hier het grondslagartikel 6 lid 1 sub d ; het vitale belang).

Binnen het sociaal domein zijn ook professionals werkzaam die vanuit hun beroepscode zijn gebonden aan een wettelijke geheimhoudingsplicht en daarnaast ook aangesteld zijn als ambtenaar. Het niet zorgvuldig omgaan met geheimhouding door professionals die vanuit hun beroepscode zijn gebonden aan een wettelijke geheimhoudingsplicht kan leiden tot een klacht bij het medisch tuchtcollege. Denk hierbij aan medewerkers met een SKJ registratie of medewerkers die vallen onder de beroepscode maatschappelijk werk. Medewerkers zonder wettelijke geheimhoudingsplicht dienen zich ook te realiseren dat het onzorgvuldig omgaan met persoonsgegevens neer kan komen op plichtverzuim. In het kader daarvan wordt bij autorisaties van medewerkers in verband met toegang tot cliëntsystemen uitdrukkelijk gewezen op de geheimhoudingsplicht en de consequenties van overtreding c.q. plichtsverzuim.

4.6 Triage
Triage betekent in het kader van de privacy, het maken van een inschatting van de grootte van het probleem of de vraag om op basis daarvan te prioriteren. Hoe minder groot het probleem of de vraag, hoe minder aanleiding er is om gegevens van betrokkene te verwerken (met de kanttekening dat je er tegelijkertijd niet aan ontkomt om in eerste instantie wel bepaalde gegevens te verwerken om de triage goed uit te kunnen voeren). Triagemomenten zijn de momenten waarop een afweging wordt gemaakt met betrekking tot de verwerking van persoonsgegevens.

De mate waarin persoonsgegevens mogen worden verzameld hangt met name af van de hulpvraag. Van daaruit wordt het doel, met het oog waarop gegevens worden verzameld, duidelijk. Gedurende het proces van 'aanvraag – verwerking – toekenning – uitvoering hulp' wordt de complexiteit van de hulpvraag duidelijk. Het is belangrijk om deze verschillende fases goed te onderscheiden, omdat tijdens het proces de hulpvraag, het doel, de taak van de medewerker gebiedsteam en de noodzaak tot het inschakelen van derden voor het bereiken van het doel kan veranderen. Met het veranderen van het doel verandert ook de mate waarin persoonsgegevens mogen worden verwerkt.

Belangrijke triagemomenten zijn:
1. Aanmelding/aanvraag
2. Brede vraagverheldering (geldt alleen binnen de gebiedsteams)
3. Opstellen beschikking en opdrachtverlening
4. Hulpverlening / uitvoering plan

Het triagekader wordt dan als volgt toegepast:
- Door middel van triage wordt bepaald waar de hulpvraag thuishoort en welke vorm van gegevensverwerking noodzakelijk is.
- De medewerker maakt een zorgvuldige afweging met betrekking tot de gegevensverwerking rondom de vraag en legt, indien deze afwijkt van hetgeen regulier is maar wel noodzakelijk, de afwegingen vast in het dossier. Betreft het meerdere domeinen dan kan dit enkel met toestemming van de inwoner als de specifieke wet- en regelgeving dit niet toestaat.
- De hulpvraag/aanvraag van de inwoner is leidend. Als in overleg met de inwoner de brede vraagverheldering plaats vindt vanuit het gebiedsteam, dan worden met toestemming van de inwoner over alle besproken domeinen gegevens verwerkt.
- De beslissingen en de triagemomenten worden onderbouwd en gedocumenteerd. Expliciet wordt vastgelegd welke afwegingen worden gemaakt en wat het resultaat is van een bepaalde afweging.

In de gemeente Súdwest-Fryslân werkt het gebiedsteam met het onderstaande werkproces. Voor andere hulpvragen en aanvragen die niet via het gebiedsteam verlopen wordt stap 2 overgeslagen. Ook wordt er niet in alle gevallen een plan opgesteld, omdat het bij het toekennen van een voorziening niet altijd noodzakelijk is.

4.7 Persoonsgegevens uitwisselen met derden
Inwoners moeten er op kunnen vertrouwen dat er zorgvuldig wordt omgegaan met hun persoonsgegevens wanneer bepaalde ondersteuning wordt ontvangen en dat dit binnen de kaders van de wet gebeurt. Hieronder volgen verschillende situaties en overlegvormen waar persoonsgegevens verwerkt kunnen worden en gedeeld met derden intern en extern.

4.7.1 Integrale dienstverlening over de domeinen heen
Als gevolg van de decentralisaties wordt van de gemeente een integrale dienstverlening verwacht. De wetgever heeft weliswaar beoogd dat meer integraal wordt samengewerkt binnen het sociaal domein

(één gezin, één plan, één regisseur), maar de wetgever heeft nagelaten deze regietaak specifiek in de wetgeving te verankeren. Ook zijn in de bijzondere wetten (Participatiewet, Wmo, Wgs en Jeugdwet) geen of slechts beperkte regels opgenomen die specifieke mogelijkheden bieden tot domeinoverstijgende gegevensdeling. Dit betekent dat er op dit moment voor de gemeente geen algemene (publiekrechtelijke) wettelijke grondslag bestaat om tussen de verschillende wetten zoals Jeugdwet, Wmo 2015, Wgs en Participatiewet, zonder meer persoonsgegevens uit te wisselen. Er is wel een wetsvoorstel, de Wams, om meer integraliteit te gaan organiseren. Op dit moment ligt het wetsvoorstel ter advies bij de Raad van State. Door met toestemming van de inwoner de brede vraagverheldering in te zetten, wordt er binnen de gebiedsteams van de gemeente wel al integraal gewerkt binnen dat deel van het Sociaal Domein.

Het kunnen delen van gegevens binnen en in sommige gevallen over domeinen heen of zelfs met externen kan echter wel noodzakelijk zijn. Deze deling vindt niet plaats voordat de betrokkene hiervoor vooraf mondeling of schriftelijk ondubbelzinnig toestemming heeft gegeven (welke wordt vastgelegd in het dossier). Indien de specifieke wetgeving het eist wordt er een toestemmingsverklaring getekend waaruit blijkt dat er toestemming is voor gegevensuitwisseling voor het betreffende moment waaruit duidelijk blijkt om welke gegevens het gaat en met welk doel ze worden verwerkt (maar zoals eerder aangegeven, dat mag geen vrijbrief zijn!). Zo is bijvoorbeeld het uitwisselen en/of bespreken van persoonsgegevens met internen die op een ander gebied binnen het sociaal domein werkzaam zijn (bijvoorbeeld tussen een Wmo-consulent en een bijstandsconsulent) niet toegestaan zonder ondubbelzinnige toestemming van de betrokkene. De betrokkene moet ook weten met welk doel de gegevens worden opgevraagd of gedeeld, wat de inhoud is van de informatie en wat mogelijke consequenties van de gegevensverstrekking zijn. Is er sprake van een bijzonder geval waarvoor bepaalde verstrekking van gegevens nodig is, wordt er een zorgvuldige afweging gemaakt. Het vragen van toestemming met het oog op de specifieke situatie is cruciaal. Voor de uitvoering van de Jeugdwet geldt dat als de betrokkene nog geen 12 jaar oud is, toestemming gevraagd wordt van de wettelijk vertegenwoordiger van de betrokkene. Voor een betrokkene met een leeftijd tussen de 12 en 16 jaar geldt een gezamenlijke vertegenwoordiging. Dit houdt in, dat zowel aan de betrokkene als aan de wettelijk vertegenwoordiger toestemming moet worden gevraagd. Is de betrokkene ouder dan 16 jaar, dan wordt er alleen toestemming gevraagd aan de betrokkene, omdat een persoon ouder dan 16 jaar zelfstandig is bevoegd.

4.7.2 Casusoverleg

Indien een casus besproken wordt in een overleg waarbij verschillende medewerkers intern en/of extern betrokken zijn dan moet bij uitwisseling van persoonsgegevens aan de AVG en de Wmo 2015, Jeugdwet, Wgs, Participatiewet en eventuele aanpalende wetgevingen worden voldaan. Artikel 5.1.1, vierde en vijfde lid, Wmo 2015 geeft een wettelijke grondslag, het regelt dat persoonsgegevens van de inwoner die zijn verkregen ten behoeve van de uitvoering van de Jeugdwet, de Participatiewet en de Wet gemeentelijke schuldhulpverlening kunnen worden gebruikt in het kader van een goede afstemming van te verlenen ondersteuning in de zin van de Wmo 2015 indien betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend.
Daarnaast is het overigens het meest wenselijk dat de betrokkene zelf bij het casusoverleg aanwezig is. Degene die als professional gegevens wil delen met een ander moet daarvoor een grondslag hebben en de noodzaak tot het delen van bepaalde gegevens met bepaalde anderen hebben vastgesteld. Het is vervolgens aan de professional om een afweging te maken of een bepaalde casus moet worden besproken met één of meer collega's en of de bespreking met anonimiteit van de betrokkenen (dus geen verwerking van persoonsgegevens) kan plaatsvinden. Terughoudendheid is hier geboden gelet op de privacywetgeving. Ook kan een bespreking in een casusoverleg anoniem plaatsvinden, waarbij geen persoonsgegevens worden gewisseld. In situaties waarin wel persoonsgegevens worden vermeld en dus een uitwisseling van deze gegevens plaatsvindt geldt tevens dat iedere uitwisseling moet worden getoetst aan de eisen van proportionaliteit (niet meer privacy inbreuk dan nodig) en subsidiariteit (ander middel dat minder inbreuk op privacy maakt om het gestelde doel te realiseren, heeft de voorkeur).

De volgende uitgangspunten worden gehanteerd met betrekking tot casusoverleggen binnen één domein, over de domeinen heen en casusoverleggen waar externen bij betrokken zijn (zorgaanbieders, politie, woningbouwverenigingen etc.):

- Uitgangspunt is dat de betrokkene aanwezig is, zo niet dan;
  - Is er toestemming gevraagd aan de betrokkene om de casus te bespreken? Is die toestemming er niet, dan mag de situatie alleen worden besproken als er sprake is van overmacht. Dat wil zeggen dat door de situatie te bespreken zonder toestemming, ernstig nadeel voor betrokkene kan worden voorkomen;
  - Is er geen toestemming dan wordt in principe de casus anoniem besproken. Pas als dat niet kan om het gewenste doel te bereiken, worden persoonsgegevens verstrekt over de casus;

- Alleen die gegevens worden ingebracht, die noodzakelijk zijn om het doel van het overleg te bereiken;
- De deelnemers aan het overleg zijn direct betrokken bij de casus;
- Het verslag van het overleg bevat afspraken en maakt onderdeel uit van het dossier, waardoor inzagerecht geldt voor de betrokkene;
- De betrokkene wordt zo spoedig mogelijk geïnformeerd over de afspraken en de uitkomsten van het casusoverleg;
- Verslaglegging naar aanleiding van een casusoverleg gebeurt alleen in het dossier van het cliëntsysteem.

Deelnemers aan een casusoverleg moeten zich realiseren dat als hun informatie eenmaal wordt gedeeld tijdens het casusoverleg en/of in het dossier komt, hierop alle privacyrechten van toepassing zijn. Betrokkene kan op elk moment zijn/haar rechten uitoefenen zoals het recht op inzage in het dossier. Als er geen toestemming kan worden gevraagd, of deze niet wordt gegeven, kan een hulp-/dienstverlener, toch cliëntgegevens aan een derde verstrekken als er sprake is van een ernstig gevaar voor de veiligheid en/of gezondheid van de betrokkene. In het kader van het transparantiebeginsel wordt dit wel gemeld aan de betrokkene. Een hulp-/dienstverlener kan op grond van noodzakelijkheid besluiten om gegevens aan een derde te verstrekken. Dergelijke handelingen worden opgenomen in het dossier, voorzien van de redenen die hebben geleid tot het besluit.

Binnen een casusoverleg is er sprake van casusregie en anderzijds procescoördinatie. Casusregie heeft betrekking op het aanspreekpunt voor de betrokkene. De casusregisseur is verantwoordelijk voor het beheer van het dossier binnen het betreffende domein en de afhandeling van inzageverzoeken in dossiers. Bij twijfel over wat er verstrekt mag worden, kan de casusregisseur de privacy officer om advies vragen. Privacyverzoeken in het kader van de AVG handelt de privacy officer af. Zie ook onder 4.10. Andere hulp-/dienstverleners binnen ditzelfde domein mogen dit dossier alleen inzien als zij zelf ook bij de casus betrokken zijn.

Procescoördinatie ziet toe op de zorgvuldigheid van het ondersteuningstraject als er hulp-/ dienstverleners vanuit meerdere onderdelen van het sociaal domein bij een casus betrokken zijn en de casus complex is of als er veel externe partners bij betrokken zijn. Hierbij wordt steeds het principe ‘1 gezin, 1 plan, 1 regisseur’ gehanteerd. De gegevens die de procescoördinator nodig heeft vanuit de verschillende onderdelen van het sociaal domein moeten actueel en betrouwbaar zijn. Een zorgvuldige verslaglegging in de dossiers door de casusregisseurs van de betreffende domeinen is daarom essentieel. Belangrijk is ook dat er snel geschakeld wordt tussen procescoördinator en betrokken hulp-/dienstverleners. De procescoördinator maakt bij onvoldoende voorhandige informatie zelf een inschatting op basis van de beschikbare informatie. In de meeste gevallen wordt er gehandeld op basis van gegevens die door de hulp-/dienstverleners zijn verwerkt zonder dat de procescoördinator zelf contact hierover heeft gehad met betrokkene. Dat vereist extra zorgvuldigheid. Casusregisseurs en andere hulp-/dienstverleners blijven ook bij procescoördinatie zelf verantwoordelijk voor hun dossier met betrekking tot de betreffende inwoner en moeten de inwoner zelf informeren als er uitwisseling van gegevens met de procescoördinator plaatsvindt.

4.7.3 Signalering en handhaving

Het bieden van ondersteuning op basis van vertrouwen kan onder druk komen te staan als gegevens worden uitgewisseld met instanties/medewerkers die in de eerste plaats toezicht of handhaving als taak hebben, zoals politie/OM, leerplichtambtenaren, medewerkers in het domein werk en inkomen (die onder andere bezig zijn met het opsporen van bijstandsfraude) Wmo en Jeugdwet (in verband met rechtmatigheidscontoles. Samenwerking met genoemde toezichthouders/handhavers kan nuttig zijn voor een goede ondersteuning en voordeel opleveren voor de betrokkene, als het hulpverleningsperspectief niet uit het oog wordt verloren. De gemeente heeft een zeer brede wettelijke taak waardoor de signalering van problemen door toezichthouders/handhavers in veel gevallen onder de gemeentelijke verantwoording valt, maar er moet bij het delen van gegevens altijd gekeken worden naar het doel waarvoor de gegevens zijn verzameld en alleen daarvoor gebruikt worden.

Wanneer mogen gegevens vanuit het sociaal domein gedeeld worden voor signalering en handhaving:

- Als de betrokkene hier toestemming voor heeft gegeven;
- Als het noodzakelijk is:
  - voor de uitvoering van de Jeugdwet, de Wmo 2015, Wgs en/of Participatiewet maar ook bij de diverse wetten zoals IOAZ, IOAW, en de gemeentelijke regeling zoals de beleidsregels

gehandicaptenparkeerkaarten en gehandicaptenparkeerplaatsen 2020 gemeente Súdwest-Fryslân;
- om te voldoen aan een wettelijke verplichting;
- om de vitale belangen van de betrokkene te beschermen;
- voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan burgemeester of aan het college is opgedragen.

Als een hulp-/dienstverlener constateert dat een cliënt in strijd handelt met bepaalde regels of zelfs strafbare feiten op het spoor komt of daarover vermoedens heeft, zonder dat dit bij handhavers bekend is, dan confronteert de hulp-/dienstverlener de betrokkene hiermee, op een dusdanige manier dat het vertrouwen van de betrokkene in de hulp-/dienstverlener niet in het gedrang komt. Dat doet hij vanuit zijn relatie als hulp-/dienstverlener. Die confrontatie biedt betrokkene de gelegenheid er zelf wat aan te doen. Als echter één van bovenstaande punten van toepassing is, dan kan de hulp-/dienstverlener die stap overslaan en direct aangifte of een melding doen bij de desbetreffende gemeentelijke afdeling of politie, bij Veilig Thuis indien sprake is van huiselijk geweld of kindermishandeling.
Er kan onderscheid gemaakt worden tussen een misdrijf dat een gevaar vormt voor de omgeving (veiligheid of gezondheid), fraude en een overtreding. Een misdrijf vormt bijna altijd een gevaar voor de omgeving en dient altijd te worden gemeld door de hulp-/dienstverlener (als de inwoner het niet zelf doet). Uitzondering hierop is als de hulp-/dienstverlener het misdrijf niet zelf heeft gezien, maar er alleen over hoort. Een hulp-/dienstverlener met een beroepscode moet een goede afweging maken of de signalen dusdanig ernstig zijn dat hij zijn wettelijke geheimhoudingsplicht gaat schenden.

4.7.4 Minderjarigen en wilsonbekwamen

Bij hulp aan minderjarigen en wilsonbekwame meerderjarigen vraagt de hulp-/dienstverlener zich altijd zelfstandig af wat uit oogpunt van ondersteuning het beste is voor het kind of de meerderjarige die niet (meer) in staat wordt geacht tot een redelijke waardering van zijn belangen (wilsonbekwame). Tevens wordt bij alle verzoeken van ouders/voogden met betrekking tot de ondersteuning en het dossier van het kind het belang en de veiligheid en/of gezondheid van het kind, afgewogen tegen het recht om geïnformeerd te worden en invulling te geven aan het ouderlijk gezag. Het is daarom belangrijk dat de hulp-/dienstverlener zich van te voren op de hoogte stelt van de gezagsrelatie tussen ouder en kind, zeker als er verschil van mening is tussen beide ouders. Op basis van de leeftijd van het kind en degenen die het gezag - wettelijke vertegenwoordiging – hebben over het kind, gaat de hulp-/dienstverlener na wie betrokken mogen en moeten worden, welke personen geïnformeerd mogen worden en van wie toestemming nodig is met betrekking tot het verwerken en/of delen van gegevens. Zelfs binnen hetzelfde gezin moet hier zorgvuldig mee worden omgegaan. Afhankelijk van de leeftijd hebben minderjarigen binnen hetzelfde gezin niet dezelfde rechten. Kinderen jonger dan 12 jaar hebben geen zelfstandige rechten. Vanaf 16 jaar mogen kinderen zelfstandig verzoeken doen. Bij de groep daar tussen in, de 12 t/m 15-jarigen, is extra zorgvuldigheid vereist. Zij kunnen bijvoorbeeld zelf verzoeken doen met betrekking tot de ondersteuning en hun dossier en bezwaar maken als hun ouders het dossier willen inzien. Het is in die gevallen aan de hulp-/dienstverlener om te beoordelen of het kind voldoende is staat is tot het nemen en overzien van die beslissingen en te beslissen of hij/zij de verzoeken van het kind wel of niet honoreert.

Voor de Participatiewet en Wmo 2015 geldt dat minderjarigen geen zelfstandig recht op bijstand of ondersteuning hebben. Eventuele bijstand of ondersteuning wordt verleend aan de ouder(s) waarvan het kind ten laste komt. Voor meerderjarige wilsonbekwame personen kan mentorschap en/of bewindvoering van toepassing zijn. De wettelijke regeling van mentorschap beoogt bescherming te bieden aan meerderjarigen die ten gevolge van hun geestelijke of lichamelijke toestand niet in staat zijn om of bemoeilijkt worden in het behartigen van hun belangen van niet-vermogensrechtelijke aard. Is er sprake van beschermingsbewind, dan mag iemand niet meer zelf beslissen over de goederen (zaken en vermogensrechten) die onder bewind staan. Zijn vermogen wordt beschermd. Keuzes op het persoonlijke vlak kan de onder bewind gestelde persoon echter nog gewoon maken.

4.7.5 Vroegsignalering

Bij vroegsignalering gaat het om de verwerking van persoonsgegevens van inwoners of gezinnen in een stadium waarin betrokkenen zelf (nog) niet om hulp of ondersteuning vragen. Wettelijke regelingen met betrekking tot de verwerking van persoonsgegevens ten behoeve van vroegsignalering zijn bijvoorbeeld vormgegeven middels de Verwijsindex risicojongeren (VIR) en Veilig Thuis. Jongeren tot 23 jaar waarover zorgen zijn of waarbij betrokkenheid is, kunnen worden geplaatst in de VIR, nadat er een mededeling is gedaan aan ouders en/of jongere. Binnen de uitvoering van de Jeugdwet wordt het signaleringsysteem Zorg voor Jeugd gehanteerd. Dit is een landelijk systeem waarop vele instanties die werken met jeugdigen zijn aangesloten. Zorg voor Jeugd is gekoppeld aan de VIR. Het systeem van

Zorg voor Jeugd is voorzien van een deugdelijke privacybescherming. Voor zover er sprake is van een publiekrechtelijke taak of een wettelijke verplichting kan daarop als grondslag een beroep worden gedaan.

De Wgs welke is ingegaan op 1 januari 2021, verplicht verhuurders van woonruimte om betalingsachterstanden van hun huurders te melden bij de gemeente waar de huurder woont. Een dergelijke verplichting gold al voor leveranciers van andere essentiële voorzieningen, zoals zorgverzekeraars, energieleveranciers en drinkwaterbedrijven. Vanaf 1 januari 2021 geldt deze wettelijke meldplicht ook voor alle verhuurders van woningen. Dus ook hier is een wettelijke grondslag om vroegtijdig signalen neer te leggen bij de gemeente.

Overige vormen van vroegsignalering zijn niet wettelijk geregeld waardoor een grondslag voor de verwerking van persoonsgegevens ontbreekt. Dit betreft bijvoorbeeld het registreren van signalen en meldingen van bezorgde professionele hulpverleners of anderen. Ook domeinoverstijgende vroegsignalering is niet wettelijk geregeld. Wel kunnen afspraken worden gemaakt met hulpverleners of anderen (bijvoorbeeld woningbouwverenigingen) dat zij inwoners wijzen op de mogelijkheden van hulpverlening door gemeenten of andere instanties. Ook outreachende hulpverlening kan een mogelijkheid bieden om de inwoner bij de juiste hulpverlenende instantie te krijgen. De gemeente Súdwest-Fryslân signaleert problemen vroegtijdig door inzet en zichtbaarheid van medewerkers in de kernen en wijken.

4.7.6 Gedwongen kader

Soms is er sprake van hulpverlening met een gedwongen karakter. Zo zijn er aparte vormen van toezicht op jongeren in de wet geregeld, die door de rechter ingesteld kunnen worden (denk aan Kinderbeschermingsmaatregelen zoals een ondertoezichtstelling en/of een machtiging tot uithuisplaatsing, of verplichte Jeugdreclassering nadat een jongere de wet heeft overtreden). Dit wordt ook wel het gedwongen kader genoemd. Er bestaan afspraken met de Raad voor de Kinderbescherming (RvdK) (die onderzoeken verricht ten behoeve van het instellen van kinderbeschermingsmaatregelen) en gecertificeerde instellingen (GI) (die dit toezicht uitvoeren en ook beslissen welke hulp wordt geboden). Deze afspraken betreffen onder andere de uitwisseling van gegevens. Voor de uitwisseling van deze gegevens tussen gemeente en RvdK/GI is geen toestemming van betrokkene nodig zolang duidelijk is dat dit noodzakelijk is voor de uitvoering van de wettelijke taak en ook de principes van proportionaliteit en subsidiariteit in acht zijn genomen. Dit geldt overigens ook voor de uitwisseling van gegevens met Veilig Thuis (regionaal advies- en meldpunt voor huiselijk geweld en kindermishandeling). Veilig Thuis is wettelijk bevoegd om zonder toestemming van de betrokkenen informatie op te vragen en te delen ten behoeve van een onderzoek, als dat noodzakelijk is voor de veiligheid, het herstel of de toekomstige ontwikkeling van de betrokkenen. Iedere organisatie en zelfstandige professional heeft een eigen meldcode Huiselijk geweld en Kindermishandeling met daarin 5 stappen. Iedere organisatie is wettelijk verplicht om deze 5 stappen in haar meldcode op te nemen. Door de meldcode te volgen kan de situatie van een inwoner gemeld worden bij Veilig Thuis. Bij de uitvoering van een advies- of consultatietaak door Veilig Thuis is het zonder toestemming opvragen van informatie niet van toepassing.

4.8 Recht op informatie

Gemeenten zijn verplicht de inwoner te informeren over het feit dat er gegevens over hem of haar worden verwerkt, wie de verantwoordelijke voor deze verwerking is en met welk doel de verwerking plaatsvindt. Deze informatieplicht is een uitwerking van het transparantiebeginsel dat is bedoeld om de betrokkenen in staat te stellen de verwerkingsverantwoordelijke (in rechte) aan te spreken. De omvang van de informatieplicht hangt af van wat nodig is om een “rechtmatige gegevensverwerking” te waarborgen en van de leeftijd van de betrokkene. Vanaf 16 jaar moeten kinderen geïnformeerd worden en kunnen zij zelfstandig handelen met betrekking tot hun gegevens. Voor kinderen tussen 12 en 15 geldt dat de hulp-/dienstverlener inschat in hoeverre het kind geïnformeerd kan worden of in staat is beslissingen te nemen met betrekking tot deze rechten.
Bij het informeren van betrokkenen is het niet voldoende te verwijzen naar algemene doelen. Algemene informatie op bijvoorbeeld de website van de gemeente is dus niet voldoende om te voldoen aan de informatieplicht. Betrokkene moet op het moment van verzamelen worden geïnformeerd, ook als het om een indirect betrokkene gaat (bijvoorbeeld persoonsgegevens van ex-partner). Uiteraard kan informatie op de websites wel worden geboden als achtergrondinformatie. Er zijn een aantal uitzonderingen op de informatieplicht, bijvoorbeeld als informeren onmogelijk blijkt of een onevenredige inspanning kost. Er is bijvoorbeeld sprake van onevenredige inspanning als de gebruikelijk manier van contact leggen geen resultaat heeft opgeleverd, vervolgens andere manieren of media om de betrokkenen te bereiken ook niets hebben opgeleverd en het heel veel tijd gaat kosten om een adres te achterhalen.
Aan het transparantiebeginsel wordt vormgegeven door actieve voorlichting aan de betrokkene en het actief aanbieden van informatie over het ondersteuningstraject. Er wordt actief, open en transparant gecommuniceerd naar de betrokkene. Voor het inrichten van deze communicatie wordt gebruik gemaakt van diverse communicatiemiddelen, te weten:

- mondeling tijdens contactmomenten;
- via de websites van de specifieke domeinen, voorzien van informatie over privacy en een privacystatement;
- via informatieve folders.

4.9 Recht op kennisgeving
De betrokkene wordt, afhankelijk van zijn/haar leeftijd, geïnformeerd als zijn/haar persoonsgegevens worden gecorrigeerd, verwijderd of beperkt. Alleen als dit onmogelijk is of onevenredig veel inspanning kost hoeft dat niet. Het dossier kan op schriftelijk verzoek in principe door de betrokkene worden ingezien.

4.10 Recht op inzage en afschrift
Betrokkenen hebben recht op inzage in hun persoonsgegevens o.g.v. artikel 15 AVG. Art 15 AVG geeft slechts het recht om een overzicht te verkrijgen van de persoonsgegevens die de gemeente van hen in bezit heeft. Dit is wat anders dan inzage verkrijgen in een geheel dossier of kopieën van het dossier verkrijgen. Inzageverzoeken in persoonsgegevens op grond van artikel 15 AVG worden behandeld door de privacy officer. Dit gaat via de gemeentelijke inzageprocedure. Er wordt hierop een besluit gegeven welke vatbaar is voor beroep.
Wil iemand inzage in zijn of haar dossier, dan gaat dit via de betrokken medewerker. Deze kan de privacy officer om advies vragen als er twijfel bestaat over wat er verstrekt mag worden. In het dossier hoeven geen werkaantekeningen te worden opgenomen. Iets is een werkaantekening als het enkel inzichtelijk is voor de medewerker en niet digitaal is opgeslagen en niet te relateren is aan een inwoner.

4.11 Recht op rectificatie
De betrokkene heeft, afhankelijk van zijn/haar leeftijd, recht op correctie als de persoonsgegevens volgens hem/haar onjuist of onvolledig zijn. Hij kan er dan voor zorgen dat de onjuiste gegevens niet langer worden gebruikt of onvolledige gegevens worden aangevuld. Deze procedure is beschreven in de gemeentelijke Procesbeschrijving verzoek tot rectificatie.
Een gemeente kan alleen persoonsgegevens rectificeren als zij zelf verantwoordelijk is voor deze gegevens. Gegevens afkomstig van derden, zullen bij de derden gerectificeerd moeten worden.

4.12 Recht op wissing van gegevens
Een betrokkene kan, afhankelijk van zijn/haar leeftijd, ook een schriftelijk verzoek doen om het dossier - of delen daarvan – te wissen. Het recht daartoe bestaat bijvoorbeeld als de persoonsgegevens niet meer nodig zijn voor de doelen waarvoor deze zijn verzameld of verwerkt, of de persoonsgegevens onrechtmatig zijn verwerkt.

Deze procedure is beschreven in de gemeentelijke Procesbeschrijving verzoek tot gegevenswissing. Nadat het schriftelijke verzoek is ingediend, moeten de betreffende gegevens worden gewist. Het wissen van gegevens hoeft niet als het bewaren van het dossier belangrijk(er) is voor een ander dan de betrokkene. Vernietiging hoeft ook niet als dat in strijd is met een wettelijke bepaling. De Archiefwet bepaalt voor verschillende dossiers van verschillende domeinen binnen de gemeente hoelang de bewaarplicht is. Deze termijnen zijn terug te vinden in de selectielijst.

Het recht op vergetelheid hangt nauw samen met het recht om gegevens te laten wissen. Bij een verzoek voor vergetelheid moet de verwerkingsverantwoordelijke er ook voor zorgen dat er geen verdere verspreiding van de gegevens plaatsvindt door anderen.

4.13 Recht op beperking van verwerking
De betrokkene heeft, afhankelijk van zijn/haar leeftijd, recht op beperking van de verwerking van persoonsgegevens. Dit is onder andere het geval als:
- de juistheid van de gegevens door de betrokkene wordt betwist;
- de verwerking onrechtmatig is, maar de betrokkene wil de gegevens niet laten wissen;
- de persoonsgegevens niet meer nodig zijn voor de verwerkingsdoelen, maar de betrokkene de gegevens nodig heeft voor de instelling, uitoefening of verdediging van een rechtsvordering.

Als de betrokkene de beperking van verwerking schriftelijk (per post of digitaal) heeft aangevraagd, maar niet wil dat de persoonsgegevens gewist worden, dan kunnen de gegevens opgeslagen blijven in het dossier zodat deze voor de betrokkene toegankelijk blijven om ze bijvoorbeeld op te kunnen vragen. Andere verrichtingen zijn niet toegestaan. Zijn verrichtingen toch gewenst of noodzakelijk, dan wordt hiervoor toestemming aan de betrokkene gevraagd.

4.14 Recht op overdraagbaarheid
Als de inwoner toestemming heeft gegeven voor het opslaan/bewerken van persoonsgegevens heeft de inwoner het recht deze persoonsgegevens aan een andere verwerkingsverantwoordelijke over te

dragen, zonder daarbij gehinderd te worden door de verwerkingsverantwoordelijke aan wie de persoonsgegevens zijn verstrekt. De inwoner kan hiertoe een verzoek indienen, waarop indien mogelijk de gegevens rechtstreeks naar de andere verantwoordelijke wordt verstuurd.

4.15 Bezwaar en klachten
Als de verwerking van persoonsgegevens berust op een grondslag uit de AVG heeft de betrokkene (afhankelijk van zijn/haar leeftijd) toch te allen tijde het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. Dit bezwaar is dus niet tegen een besluit, maar tegen de verwerking van de persoonsgegevens. Als de betrokkene een schriftelijk bezwaar indient dan wordt hierop wel een besluit genomen waartegen wel bezwaar open staat in de zin van de Awb. De verwerking van de persoonsgegevens stopt, tenzij er gerechtvaardigde gronden zijn voor de verwerking. Vervolgens wordt bekeken of de gegevensverwerking op een juiste manier heeft plaatsgevonden.
Naast het indienen van bezwaar tegen de verwerking van persoonsgegevens is het ook voor iedere betrokkene mogelijk om een klacht in te dienen. Dit kan als hij meent dat zijn persoonsgegevens zijn verwerkt in strijd met de wet. Het indienen van een klacht gebeurt bij de Autoriteit Persoonsgegevens. Het gaat hier niet om een klacht in de zin van de Awb, maar een verzoek tot handhaving aan de Autoriteit persoonsgegevens. De schriftelijke reactie van de Autoriteit persoonsgegevens hierop is een besluit in de zin van de Awb, waartegen rechtsbescherming open staat langs de gebruikelijke bestuursrechtelijke weg. Het stoppen met het verwerken van persoonsgegevens als gevolg van het indienen van een bezwaar of klacht kan als gevolg hebben dat de uitvoering van de ondersteuning ingeperkt moet worden of helemaal gestopt moet worden.

4.16 Recht op menselijke blik
Organisaties kunnen besluiten over mensen nemen op basis van automatisch verwerkte gegevens. Het is dan niet een persoon die het besluit neemt, maar de computer. Ook bij de besluitvorming binnen het sociaal domein zou dat kunnen gaan spelen, bijvoorbeeld bij het herontwerpen van processen. Nu is dat nog niet het geval.

Nieuw besluit
De AVG geeft het recht te vragen om een menselijke blik bij automatisch genomen besluiten. Dat betekent dat de gemeente een nieuw besluit moet nemen waarbij een mens uw gegevens heeft beoordeeld. Dit staat omschreven in artikel 22 AVG lid 1. "De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft."

Voorwaarden automatisch besluit
De gemeente mag alleen een automatisch besluit nemen in een van de volgende gevallen:
- Er een overeenkomst met de betrokkene hierover is afgesloten;
- Er staat in een wet dat het mag;
- De betrokkene uitdrukkelijk toestemming heeft gegeven.

Bij het nemen van automatische besluiten nemen is het van belang systemen regelmatig te controleren en te testen op een correcte werking en juiste resultaten.

5. Beheer en opslag gegevens

In dit hoofdstuk is beschreven hoe we omgaan met de gegevens die in digitale systemen of fysiek zijn opgeslagen.

5.1 Gegevensopslag in dossiers
Binnen het sociaal domein worden gegevens opgenomen in cliëntdossiers, in verschillende digitale systemen en in beperkte mate in dossierkasten binnen het betreffende domein, of in het archief. De gegevens kunnen afkomstig zijn van de inwoner zelf of afkomstig zijn één van de basisregistraties. In de Basisregistratie Personen (BRP) worden gegevens bijgehouden van iedereen die in Nederland woont. De gegevens uit de BRP worden gebruikt om de taken in het kader van het sociaal domein te kunnen uitvoeren. De gegevens worden daarvoor aangevuld met andere gegevens en vastgelegd in andere systemen ten behoeve van deze taken. Op deze registraties is de AVG van toepassing. Voor de uitvoering van de taken binnen het sociaal domein wordt gebruik gemaakt van een backoffice systeem. Deze zijn voorzien van zeer strenge functie gerelateerde autorisaties. Suites voor het Sociaal Domein bestaat uit meerdere onderdelen. De applicatie Suite4SociaalDomein bestaat uit: Suite4Zorg (Wmo), Suite4Jeugdzorg (Jeugdwet) en Suite4inkomen (Participatiewet). Suite4SocialeRegie is een vrij nieuwe en overkoe-

pelende module, specifiek voor de toegang. Deze Suites worden gebruikt door verschillende toegangen van gemeenten. Ook hiervoor geldt dat de verwerking voldoet aan alle privacyregels.

Naast Suites wordt voor de uitvoering van de Participatiewet Suwinet gebruikt. De Gemeenschappelijke elektronische Voorziening Suwi is een elektronische infrastructuur die is ontwikkeld om ervoor te zorgen dat de Suwi-ketenpartijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak. Er worden alleen gegevens uitgewisseld wanneer er een wettelijke grondslag en doelbinding voor is. De beheerder is BKWI (Bureau Keteninformatisering Werk en Inkomen).

Als regiesysteem wordt Gidso gebruikt. Gidso is een product dat staat voor verbinden en samenwerken. De vroegsignalering, triage, regievoering, en effectmeting wordt door Gidso ondersteund. De verwerking van de persoonsgegevens van de inwoners voldoet aan alle privacy regels.

Uitgangspunten die we hanteren met betrekking tot dossiers:
- Cliëntgegevens worden bewaard in een digitaal en/of fysiek dossier;
- Als meerdere personen binnen één cliëntsysteem ondersteuning ontvangen, dan kan er een gezamenlijk dossier aangemaakt worden, mits hiervoor toestemming is verleend;
- Cliëntgegevens zijn zodanig geordend dat zij toegankelijk zijn voor de cliënt voor inzage, correctie en toevoeging;
- Cliëntgegevens zijn zodanig geordend dat zij toegankelijk zijn voor de medewerkers die bij de dienstverlening aan de cliënt of het cliëntsysteem betrokken zijn;
- Alleen de betrokken medewerkers hebben toegang tot het dossier;
- De hulp-/dienstverleners en de medewerkers van de ondersteunende diensten dragen er zorg voor dat alle relevante cliëntgegevens die hen ter kennis komen, zo snel mogelijk worden opgenomen in het dossier.

5.2 Gegevensopslag in een gegevensmagazijn Sociaal Domein
Voor het uitvoeren van onze taken en het verbeteren van onze dienstverlening gebruikt de gemeente persoonsgegevens uit relevante vakapplicaties en basisregistraties. Voor het verder professionaliseren en verbeteren van onze dienstverlening maar ook voor het in control zijn op onze processen en geldstromen is het gewenst dat we deze persoonsgegevens gaan opnemen in een gegevensmagazijn. Voor ieder doel waar wij persoonsgegevens voor willen gaan ontsluiten naar het gegevensmagazijn zal vooraf getoetst worden welke gegevens er exact worden gebruikt, de doelbinding en noodzaak van het gebruik, de verwerkingsgrondslag, en wordt waar nodig een data protection impact assessment (DPIA) uitgevoerd.
Wanneer de verwerking van de persoonsgegevens voldoet aan bovenstaande toetsing dan wordt de verwerking toegevoegd aan het verwerkingsregister.

5.3 Bewaren en vernietigen dossier
Gemeenten zijn verplicht hun dossiers en archiefbescheiden conform de Archiefwet 1995 op te slaan. Gelet op de groeiende hoeveelheid papieren en digitale informatie is het uitgangspunt van de Archiefwet dat informatie na verloop van tijd wordt vernietigd, tenzij de informatie blijvend van belang is. Actieve dossiers rondom jeugdhulp zijn digitaal opgeslagen in de Suites. Een dossier jeugdhulp wordt twintig jaar bewaard. Deze termijn begint te lopen vanaf het tijdstip waarop de laatste wijziging in het dossier heeft plaatsgevonden. Na afloop van de twintig jaar zorgt de verwerkingsverantwoordelijke voor vernietiging van de gegevens uit zowel de fysieke als de digitale dossiers. De uitvoering daarvan gebeurt door applicatiebeheer, na controle door de organisatie en de gemeentearchivaris. De termijn van twintig jaar kan worden verlengd als dat nodig is voor zorgvuldige hulpverlening. De gegevens worden ook niet vernietigd als er door of met betrekking tot een betrokkene vóór die datum een klacht is ingediend bij de gemeente of een gerechtelijke procedure is aangespannen tegen of door de gemeente met betrekking tot de ondersteuning vanuit de jeugdwet. Na afhandeling van de klacht, of na afloop van de gerechtelijke procedure, vindt vernietiging alsnog plaats. Voor jeugdbescherming, jeugdreclassering en dossiers van de Raad voor de Kinderbescherming gelden uitzonderingen. Dossiers kunnen wel eerder worden afgesloten, maar niet verwijderd. Cliënten moeten immers na afsluiting van de hulpverlening het dossier nog wel kunnen inzien of opvragen.

In de Wmo 2015 is een bewaartermijn van vijftien jaar na beëindiging van voorziening bepaald. Volgens de Selectielijst 2020, gebaseerd op de Archiefwet en het Archiefbesluit, geldt voor de Participatiewet het volgende:
Voor een uitkering of inkomensvoorziening, zoals een bijstandsuitkering, geldt een bewaartermijn van tien jaar na beëindiging. Voor eenmalige bijstandsuitkeringen, zoals bijstand voor de aanschaf van een koelkast of een computer of bijstand in de vorm van vergoedingen voor een tandartsbezoek, geldt dat deze bewaartermijn onmiddellijk aanvangt. Het is dus niet nodig deze incidentele verstrekkingen te bewaren tot na het einde van de voortdurende periodieke bijstandsuitkering. Voor een geweigerde

voorziening is de bewaartermijn vijf jaar. Er bestaat geen onderscheid tussen algemene en bijzondere bijstand. De bevoegdheid tot het verkorten van de bewaartermijn is komen te vervallen. Onderzoeken die gericht zijn op de rechtmatigheid van de bijstand of de financiële situatie van de uitkeringsgerechtigde, dienen na tien jaar vernietigd te worden.
Een korte samenvatting voor de Participatiewet op grond van de Selectielijst 2020:

Periodieke bijstand :	tien jaar na beëindiging van bijstand
Incidentele bijstand :	tien jaar na toekenning
Geweigerde bijstand :	vijf jaar na weigering
Rechtmatigheidsonderzoeken:	tien jaar na onderzoek
Terug- en invordering :	zeven jaar na inning

Beëindigde dossiers Wmo en Participatiewet gaan in het jaar na de beëindiging van de dienstverlening naar het archief. Vernietiging van het fysieke dossier vindt plaats door het Gemeentearchief.
De wettelijke regels vanuit Wmo 2015 en de Participatiewet gelden ook voor de digitale dossiers Wmo en Participatiewet.

Voor de Tijdelijke Overbruggingsregeling Zelfstandige Ondernemers (TOZO) geldt voor het aanvraagformulier een bewaartermijn van 10 jaar. Voor alle andere regelingen is er geen bewaartermijn in de Archiefwet opgenomen, wat betekent dat de gemeente zelf de bewaartermijn mag bepalen.

5.4 Beveiliging

We willen veilig omgaan met de gegevens van de inwoners. Er worden daarom permanent maatregelen uitgevoerd om bedreigingen van buitenaf voor te zijn en risico's te verminderen. Naast technische maatregelen is het creëren van bewustzijn van informatiebeveiliging bij medewerkers een belangrijk aandachtspunt.

Ook willen we voorkomen dat we inwoners onnodig lastig vallen met het vragen naar informatie waarover wij al in onze systemen beschikken. De al beschikbare informatie wordt echter alleen geraadpleegd nadat daar toestemming voor is gekregen van de betrokkene. Heeft de betrokkene toestemming gegeven, dan kan de informatie uit andere systemen worden geraadpleegd en verder verwerkt. Dit vergt het nodige van onze systemen en betekent dat we al verstrekte/verwerkte informatie van betrokkene gemakkelijk moeten kunnen vinden. De architectuur van de informatiesystemen is vastgelegd in het informatiebeveiligingsbeleid en -plan. Hierbij wordt gestreefd naar een manier van verwerken van gegevens waarbij die gegevens gemakkelijk vindbaar zijn en tegelijkertijd goed beveiligd zijn.
We houden rekening met doelbinding en hebben een goed doordacht toezicht op basis van autorisaties. Beveiligingsincidenten (of mogelijke beveiligingsincidenten) worden benaderd en afgehandeld volgens het gemeentelijke protocol ten behoeve van datalekken.

6. Governance

Governance richt zich op de inrichting van de organisatie met betrekking tot het waarborgen van de privacy van inwoners. Denk hierbij aan rollen en verantwoordelijkheden, wie voert de regie, wie controleert en hoe wordt verantwoording afgelegd. In dit hoofdstuk is beschreven wie waarvoor verantwoordelijk is en hoe er verantwoording wordt afgelegd.

6.1 Bevoegdheden en verantwoordelijkheden

Het college van B&W is verantwoordelijk voor de zorgvuldigheid van de gegevensverwerking die door of namens de gemeente plaatsvindt. Zij stelt eisen aan beveiliging en borging van de privacy. Het college van B&W is verantwoording verschuldigd aan de gemeenteraad voor de manier waarop het hieraan invulling geeft.

Taken en bevoegdheden (in willekeurige volgorde) met betrekking tot privacy binnen het sociaal domein:

- **Gemeenteraad**

De gemeenteraad controleert het college van B&W op haar verantwoordelijkheid betreffende de zorgvuldige verwerking van persoonsgegevens door de gemeente.

- **College van B&W**

Het college van B&W van de gemeente Súdwest-Fryslân is de 'verantwoordelijke' in de zin van de Algemene Verordening Gegevensbescherming (AVG). Zij is verantwoordelijk voor alles wat te maken heeft met de bescherming van persoonsgegevens binnen de gemeente. Het college stelt de kaders ten aanzien van privacybescherming en informatiebeveiliging op basis van landelijke en Europese wet- en

regelgeving en landelijke normenkaders. Het college is verantwoordelijk voor een duidelijk te volgen privacy- en informatiebeveiligingsbeleid en stimuleert het management van de organisatieonderdelen om maatregelen te nemen om persoonsgegevens van betrokkenen te beschermen en beveiligen. Het college heeft de verantwoordelijkheden op het gebied van privacybescherming en informatieveiligheid gemandateerd aan de algemeen directeur.

- **Gemeentesecretaris (Algemeen directeur)**

De gemandateerde verantwoordelijkheid voor privacybescherming en informatieveiligheid ligt bij de gemeentesecretaris. Deze stelt met het managementteam het gewenste niveau van informatieveiligheid en privacy vast voor de gemeente. Daarnaast is de gemeentesecretaris verantwoordelijk voor de juiste en volledige implementatie van de privacywet- en regelgeving en wijst voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan.

- **Procesverantwoordelijke voor de persoonsgegevens**

De procesverantwoordelijke voor de betreffende persoonsgegevens binnen de organisatie is verantwoordelijk voor de integriteit (juistheid, tijdigheid en volledigheid), de vertrouwelijkheid (waardoor de persoonsverwerking uitsluitend toegankelijk is voor daartoe geautoriseerde personen) en beschikbaarheid (het bereikbaar en inzichtelijk zijn) van de betreffende persoonsverwerking. De eigenaar is de manager of proceseigenaar van het organisatieonderdeel dat de betreffende persoonsgegevens verwerkt. De eigenaar heeft in ieder geval de volgende verantwoordelijkheden:
- Aanmelden verwerking van persoonsgegevens bij de privacy officer (PO). Wijzigingen in de verwerking van persoonsgegevens doorgeven aan de PO;
- De aanvraag, inbreng van inhoudelijke, functionele kennis, en uitvoer en effectueren van de resultaten van een data protection impact assessment (DPIA);
- Afsluiten, beheren en actualiseren van verwerkersovereenkomsten en afspraken met derden;
- Aanwijzen contactpersoon informatieveiligheid en privacy;
- Inventariseren van feiten en omstandigheden in het geval van een veiligheidsincident;
- De adviezen uit rapportages veiligheidsincidenten implementeren;
- Het belang van informatieveiligheid en privacy procedures (periodiek) onder de aandacht brengen van de afdeling; en
- Uitvoeren van het beleid ten aanzien van de betreffende persoonsgegevens die onder zijn verantwoordelijkheid vallen.

- **De functionaris gegevensbescherming (FG)**:
  - Informeert en adviseert de gemeente en de verwerkers die namens de gemeente persoonsgegevens verwerken over hun verplichtingen volgens de AVG;
  - Bevordert het privacybewustzijn binnen de organisatie;
  - Ziet toe op naleving van AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
  - Ziet toe op naleving van het gemeentelijke beleid met betrekking tot de bescherming van persoonsgegevens;
  - Ziet toe op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
  - Adviseert met betrekking tot vraagstukken over de verwerking van persoonsgegevens;
  - Adviseert met betrekking tot veiligheidsincidenten met persoonsgegevens;
  - Verzorgt meldingen en intrekkingen van meldingen datalekken bij de Autoriteit Persoonsgegevens;
  - Adviseert met betrekking tot de Privacy Impact Assessment (PIA) en het toezien of de uitvoering daarvan in overeenstemming is met de AVG;
  - Ziet toe op en adviseert over de afhandeling van vragen en klachten over het gebruik van persoonsgegevens;
  - Adviseert en ondersteunt bij het opstellen van privacynormen, produre-, -beleid, -regelingen of –gedragscodes;
  - Rapporteert rechtstreeks aan directie en het college van B&W;
  - Coördineert de privacywerkzaamheden;
  - Afstemming met de Autoriteit Persoonsgegevens; en
  - Is aanspreekpunt voor de Autoriteit Persoonsgegevens.

- **De hulp-/dienstverlener (bijvoorbeeld de medewerker gebiedsteam, de administratie SD of Ondersteuning SD)**

- Verwerkt de voor de hulpvraag benodigde gegevens;
- Verwerkt die gegevens die noodzakelijk zijn voor de uitvoering van de ondersteuning;
- Gaat zorgvuldig met persoonsgegevens om en maakt hierin afwegingen d.m.v. triage;
- Beheert en verwerkt de gegevens overeenkomstig de bepalingen van de AVG, de van toepassing zijnde materiewetgeving en dit Privacybeleid Sociaal domein;
- Zorgt voor toestemming van de betrokkene voor het verwerken van gegevens.

- **De medewerker ondersteunende diensten**

Heeft afhankelijk van zijn functie taken en verantwoordelijkheden. Medewerkers informatiebeveiliging zorgen bijvoorbeeld voor de technische beveiliging van cliëntgegevens. Hiertoe behoort ook het opstellen van een informatiebeveiligingsplan, het bewaken daarvan en het adviseren van het college over beveiliging, mogelijke risico's en de daarbij horende maatregelen. Applicatiebeheerders zijn verantwoordelijk voor het functioneel beheer van de systeemapplicaties en voeren het beveiligingsbeleid uit. Zij regelen en houden toezicht op de autorisaties. Ook zorgen zij voor het opschonen of verwijderen van cliëntdossiers na afloop van de wettelijke bewaartermijn. Juridisch medewerkers adviseren bij klachten m.b.t. privacy etc. Daarnaast zijn er nog diverse andere functies die ondersteunende werkzaamheden verrichten voor de hulp/dienstverleners.

- **De Privacy Officer (PO)**

Deze rol is gericht op de uitvoering, advisering en de naleving van de privacy wetgeving. De privacy officer adviseert over privacybescherming en over activiteiten ter bescherming van persoonsgegevens. De privacy officer heeft in ieder geval de volgende taken:
- Het beoordelen van de verwerking van persoonsgegevens tegen de achtergrond van de kaders van de (Europese)privacywetgeving. De privacy officer adviseert directie, afdelings- en teamhoofden bij wijzigingen in procesuitvoering en bedrijfsvoering en de toepassing van een DPIA;
- Als adviseur deelnemen aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens;
- Uitleg geven van de privacyvoorschriften uit de (Europese) privacywetgeving en in de sectorale wetgeving;
- Coördineren, samenvoegen en openbaar maken van de overzichten van gegevensverwerkingen die worden aangeleverd door de organisatieonderdelen van de gemeente (verantwoordelijk voor het register van verwerkingen);
- Coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
- Beheer en onderhoud van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen;
- Advisering en ondersteuning bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten, convenanten en de vaststelling van reglementen;
- Bijdragen aan privacybewustzijn;
- Opstellen privacybeleid;
- Uitvoeren van DPIA's.

6.2 Interne verantwoording
De functionaris gegevensbescherming (FG) brengt jaarlijks verslag uit aan het college met betrekking tot de bescherming van gegevens. Daarnaast ontvangt het college informatie vanuit het sociaal domein in de vorm van diverse (beheer)rapportages. Op die manier voert het college de interne controle (het onderdeel 'check') uit en kan zij de bevindingen omzetten in verbeteracties. Het college informeert de gemeenteraad vervolgens over haar bevindingen waarmee de uitvoering zichtbaar en controleerbaar plaatsvindt.

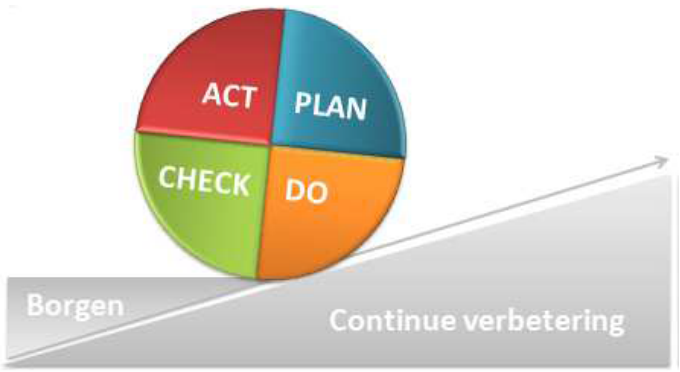
6.3 Externe verantwoording
De AVG stelt nadere eisen aan het uitbesteden van de verwerking van persoonsgegevens. De colleges van B&W dienen als verwerkingsverantwoordelijke een schriftelijke overeenkomst af te sluiten met de verwerker, in dit geval de derde partij. Deze overeenkomst heet een verwerkersovereenkomst. Het opstellen van een verwerkersovereenkomst is bedoeld om te waarborgen dat de verplichtingen die vanuit de AVG op de verwerkingsverantwoordelijke rusten, ook door de verwerker worden nageleefd. In de verwerkersovereenkomst staan afspraken en maatregelen die de verantwoordelijke genomen wil hebben door de verwerker. Belangrijk is dat volgens de AVG de verwerkingsverantwoordelijke wel aanspreekbaar blijft voor de gegevens die onder zijn verantwoordelijkheid door de verwerker worden verwerkt.
Een verwerkersovereenkomst is niet van toepassing als de verwerker kan worden gedefinieerd als een verwerkingsverantwoordelijke in de zin van de AVG. Zorgaanbieders die op zichzelf een wettelijke taak

uitoefenen en aanbieders van maatwerkvoorzieningen zijn hier voorbeelden van. Deze partijen zijn dus geen verwerker in de zin van de AVG, waardoor er ook geen verwerkersovereenkomst nodig is.
De verwerkingsverantwoordelijke dient passende en aantoonbare technische en organisatorische maatregelen uit te voeren om ervoor te zorgen dat de verwerking van persoonsgegevens in overeenstemming is met geldende wet- en regelgeving en daarover transparant te zijn. De verwerkingsverantwoordelijke moet hierover verantwoording af kunnen leggen en kan gecontroleerd worden door de Autoriteit Persoonsgegevens. Het is van belang goede afspraken te maken met de verwerker zodat de verwerkingsverantwoordelijke aan zijn wettelijke verplichtingen kan voldoen. Bijvoorbeeld over het afleggen van verantwoording en het mogelijk verrichten van controles door de functionaris gegevensbescherming.

Bovenstaande betekent dat duidelijk moet zijn aan wie welke taken worden uitbesteed door het college en dat er documentatie moet zijn waarin alle aspecten van de verwerking van persoonsgegevens door de verwerkingsverantwoordelijke is beschreven.

6.4 Privacymanagement

Het voeren van een deugdelijk privacymanagement vormt de basis als het gaat om bewustwording met betrekking tot privacy onder de betrokken medewerkers. Duidelijke visie en rollen, taken en bevoegdheden op het gebied van privacy, zoals weergegeven in dit beleid, weerspiegelen het privacymanagement. Dit stelt de verantwoordelijken in staat op een professionele manier verantwoording af te leggen omtrent privacy in het kader van de verwerking van persoonsgegevens. De plan- do- check-act cyclus speelt een grote rol in het privacymanagement van de gemeente.



Dit privacybeleid vormt het onderdeel ‘plan’.
Iedere medewerker binnen het sociaal domein is belast met het onderdeel ‘do’.
De verwerkingsverantwoordelijke draagt zorg voor de ‘check’ als onderdeel van de interne controle, waarbinnen bijvoorbeeld kwaliteitscontroles kunnen plaatsvinden gericht op privacy.
De verwerkingsverantwoordelijke draagt ook zorg voor de ‘acties’. De hulp-/dienstverleners geven uitvoering aan de acties.

7. Tot slot

7.1 Bewustwording medewerkers

Het privacybeleid wordt onder de aandacht gehouden van de medewerkers binnen het sociaal domein door het consistent verschaffen van informatie en zorgdragen voor bewustwording met betrekking tot privacy onder medewerkers. Alle interne en externe medewerkers krijgen bij aanvang van de werkzaamheden een korte introductie waarbij onder andere ingegaan wordt op privacy en de daarmee samenhangende integriteits- en geheimhoudingsverklaring die ondertekend dient te worden. Dit is echter nog niet gestandaardiseerd. Het privacy aspect is tevens geïmplementeerd in het professionaliseringstraject van de interne en externe medewerkers. Daarnaast is er aandacht voor privacy en triage in de werkprocessen en overleggen.

7.2 Bijlagen

De volgende documenten worden als bijlage opgenomen bij Privacybeleid Sociaal Domein 2023 gemeente Súdwest-Fryslân:

- Bijlage I: Visie omtrent de brede vraagverheldering geldend voor de gebiedsteams
- Bijlage II: Verwerkingsgrondslagen AVG Sociaal Domein.

7.3 Inwerkingtreding en citeertitel

1. Deze beleidsregels worden aangehaald als: Privacybeleid Sociaal Domein 2023 gemeente Súdwest-Fryslân.
2. Het Privacybeleid Sociaal Domein 2023 gemeente Súdwest-Fryslân treedt in werking de dag volgend op de bekendmaking.

Aldus vastgesteld in de vergadering van het college van 11 april 2023,
Mr. drs. J.A. de Vries, burgemeester
Drs. E.K. Strijker, gemeentesecretaris