Privacybeleid gemeente Meppel
2020-2023

Versie: 1.0
Datum: 25-2-2020

Inhoud

1. Begrippen

Betrokkene
Burgers van wie de gemeente Meppel in het kader van haar taken persoonsgegevens verzameld alsmede medewerkers in dienst van de gemeente Meppel, worden als betrokkenen aangemerkt.

Verwerkingen
Alle handelingen die een organisatie kan uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen. De gemeente Meppel verwerkt bijvoorbeeld gegevens door deze gedurende een bepaalde bewaartermijn op te slaan, waar nodig intern uit te wisselen, te wijzigen of na een beoordeling uit te wisselen met derden.

Verwerkingsverantwoordelijke
De verwerkingsverantwoordelijke is een persoon of een organisatie die het doel van en de middelen voor het gebruik van persoonsgegevens bepaalt. De gemeente Meppel is de verwerkingsverantwoordelijke voor de persoonsgegevens die zij in het kader van haar publiekrechtelijke taak verwerkt en die zij als werkgever verwerkt. In bepaalde gevallen kan de gemeente ook privaatrechtelijk handelen.

Verwerker
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Als verwerker voor de gemeente Meppel worden onder meer aangemerkt partijen die bepaalde softwarepakketten leveren.

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens volgens de AVG.

DPIA
Een DPIA is een instrument om van voorgenomen regelgeving of projecten waarbij persoonsgegevens worden verwerkt, de effecten voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen. Op basis hiervan worden maatregelen getroffen om deze effecten voor betrokkenen te voorkomen of verkleinen**.** De gemeente Meppel maakt gebruik van het model gegevensbeschermingseffectbeoordeling van de rijksdienst. Dit model is gebaseerd op de Europese regelgeving (AVG).

Datalek
Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Of zonder dat dit wettelijk is toegestaan. Er zijn drie categorieën datalekken te onderscheiden. Inbreuk op de vertrouwelijkheid, inbreuk op de integriteit en inbreuk op de beschikbaarheid. Een datalek kan, afhankelijk van de omstandigheden, in meer dan één van deze drie categorieën vallen.

Verwerkersovereenkomst
Als verwerkersverantwoordelijke is de gemeente Meppel verplicht een verwerkersovereenkomst af te sluiten met alle opdrachtnemers die namens ons persoonsgegevens verwerken. Dit kan een partij zijn die voor ons verzuimcontroles binnen de participatiewet uitvoert. Maar ook software leveranciers waar wij persoonsgegevens bij opslaan zijn verwerkers.

De verwerkersovereenkomst bevat een eenduidig pakket aan afspraken over het verwerken van persoonsgegevens tussen de gemeente Meppel als opdrachtgever en onze opdrachtnemers (ICT-leveranciers of partijen die diensten leveren).

2. Inleiding

De gemeente Meppel vindt privacy belangrijk. Dat betekent dat wij met aandacht en respect voor de privacy van bewoners en medewerkers ons werk doen. Hierom stellen we een privacybeleid vast. Ook de wet (de Algemene Verordening Gegevensbescherming, hierna: AVG) schrijft voor dat een gemeente een privacybeleid heeft. Daarmee maken we ons handelen transparant en nemen wij verantwoordelijkheid. Het beleid is geschreven voor onze inwoners, onszelf en onze medewerkers en ziet op de (onderdelen van de) gemeente Meppel als bestuursorgaan en als werkgever.

Het bestuur, Directieteam en teammanagers spelen een cruciale rol bij het waarborgen van privacy. Met dit beleid geven we een duidelijke richting aan privacy en laten we zien dat we de privacy borgen. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Het is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

Het privacybeleid is gebaseerd op de volgende (bestuurlijke) uitgangspunten en gemeentelijke kernwaarden. Deze uitgangspunten en waarden versterken elkaar.

A. Bedoeling centraal
   We zetten de bedoeling van de vraagstukken centraal bij onze verwerkingen. We doen wat nodig is voor de inwoner. We zijn transparant over onze verwerkingen zodat iedereen weet waar hij aan toe is. We handelen vanuit de geest van de wet en weten wanneer de wet strikt is.
B. Betrouwbaar Partnerschap
   De uitvoering van wettelijke taken van de gemeente, optimale dienstverlening en privacybescherming betekenen het constant zoeken naar een evenwichtige balans. Waar dit botst verantwoorden we ons over waarom we persoonsgegevens verwerken en zijn transparant in onze communicatie. We leggen eigenaarschap vast bij onze verwerkingen.
C. Samen Flexibel aan de slag
   Wendbaar, flexibel en slagvaardig werken betekend dat de basis op orde moet zijn. We gebruiken de privacywetgeving om structuren en systemen ondersteunend te maken en overbodige drempels weg te halen.
D. Juiste grondslag
   We verwerken persoonsgegevens in beginsel op basis van grondslagen die bij onze rol als gemeente horen (Wettelijke verplichting, taak van Algemeen belang en / of in het kader van een taak van Openbaar gezag).

Het beleid loopt van 2020 tot en met 2023 en wordt gelijktijdig met het Informatiebeveiligingsbeleid herzien.

2.1 Achtergrond van het beleid

Nu de AVG inmiddels meer dan een jaar geldt, is een nieuwe fase aangebroken, waarin behoefte bestaat de ruimte te nemen die de wet- en regelgeving bieden om onze taken effectief en efficiënt te vervullen en tegelijkertijd burgers met respect, eerlijk en begripvol te behandelen. Daarbij ontstaan (ethische) dilemma's. De (nationale) wet- en regelgeving is namelijk complex en biedt niet altijd voldoende houvast aan lokale beleidsmakers en –uitvoerders bij de uitvoering van hun taken. Verder heeft het recht op bescherming van persoonsgegevens geen absolute gelding en moet worden beschouwd in relatie tot de functie ervan in de samenleving. Dat vraagt soms afweging tegen andere (grond)rechten, bijvoorbeeld in het sociaal domein, waar de Rijksoverheid ons een opdracht heeft gegeven om integraal en domein overschrijdend te werken. Sommige opdrachten kunnen met elkaar botsen en soms voldoen bestaande (IT-)systemen en werkwijzen nog niet aan de privacy- en informatiebeveiligingseisen.

Privacy vraagt daarmee niet alleen om een heldere bestuurlijke visie op privacy maar ook om duidelijke beleidskaders. Privacywetgeving, waaronder de AVG, biedt niet voor ieder vraagstuk een pasklaar antwoord maar schept juist ruimte door regels in de vorm van principes te formuleren waar aan moet worden getoetst wanneer gegevens verwerkt worden. Deze regels kunnen vaak verschillend worden ingevuld of toegepast. Een belangrijk onderdeel van het beleid is aandacht voor risico oriëntatie en het moreel kompas: de wet is een belangrijke leidraad, maar bij handelen conform de regels of gebruikmaken van de (wettelijke) ruimte, hoort een gewetensvraag: ook al houd ik me aan de regels, is deze oplossing ook in maatschappelijk opzicht wenselijk? Of op de

juiste wijze invulling is gegeven aan deze principes en voldoende waarborgen zijn getroffen om de persoonlijke levenssfeer te beschermen is aan de toezichthouder en aan de rechter. De gemeente Meppel wil met dit beleid de ruimte benutten die er is om haar taken goed uit kunnen voeren en de privacy van betrokkenen beschermen. Waar dit schuurt maken wij dat transparant. Verantwoording afleggen vinden wij horen bij een betrouwbare overheid. Incorporatie van een goede privacybescherming hoort thuis in de werkzaamheden van de organisatie.

Uit het voorgaande moge duidelijk zijn dat er onduidelijkheid kan zijn over de eisen die wet- en regelgeving stellen. Dit kan tot onzekerheid leiden en medewerkers kunnen zich gehinderd voelen om hun taken uit te voeren en of privacy ervaren als een vervelende extra check bij reguliere processen. Anderen voeren – vaak ten onrechte – privacyregels juist aan om informatie niet te delen. Iets om je achter te verschuilen. Iedereen is het er echter over eens dat van ons als gemeente verwacht mag worden dat we met aandacht voor de bescherming van privacy ons werk doen. Dit beleid beoogt om de professionals op de werkvloer in staat te stellen afwegingen te maken bij de uitvoering van het werk. We willen dat rechtmatige verwerking van gegevens geen extra belastende handeling vormt maar onderdeel is van de reguliere taken en processen.

In de gemeentelijke organisatie zijn de bevoegdheden zo laag mogelijk in de organisatie belegd waarbij iedereen verantwoordelijkheid draagt voor zijn eigen taakveld, op basis van vertrouwen. Dat betekent ook dat afwegingen rond privacy, zeker als deze meer en meer onderdeel worden van de reguliere taken en processen, ook gemaakt (zullen) worden op uitvoerend niveau. Om dit soort afwegingen te kunnen maken en uit te kunnen leggen (transparantie) is een afwegingskader nodig. Hier is ook behoefte aan.

2.2 Context en reikwijdte

Dit privacybeleid bevat de domein overstijgende richtlijnen over hoe de bescherming van persoonsgegevens binnen de gemeentelijke organisatie wordt vormgegeven en georganiseerd. Het richt zich op een ieder die binnen de gemeentelijke organisatie persoonsgegevens verwerkt. Het maakt daarbij niet uit of iemand zelf bestuurder c.q verwerkingsverantwoordelijke is, medewerker in (al dan niet vaste) dienst is of krachtens een (tijdelijke) overeenkomst werkzaamheden verricht. Het beleid is van toepassing op alle verwerkingen van persoonsgegevens door/binnen de gemeentelijke organisatie, ongeacht hoe of waarop deze plaatsvindt.

Het Privacybeleid hangt samen met het Informatiebeveiligingsbeleid, waarbij de beleidsvelden samenkomen rond de beveiliging van persoonsgegevens. Deze relatie is visueel als volgt:

De AVG eist een passende beveiliging van persoonsgegevens. Ook andere gegevens moeten echter goed beveiligd worden; denk aan bedrijfsgegevens die een rechtspersoon vertrouwelijk aan de

gemeente geeft in het kader van een af te sluiten overeenkomst. Denk ook aan de eigen financiële gegevens vóórdat ze via de begroting aan de gemeenteraad worden verstrekt. Er is daarom een apart gemeentelijk informatiebeveiligingsbeleid (IB-beleid) dat ziet op de beveiliging van alle gegevens, of het nu persoonsgegevens zijn of niet.

3. Beginselen AVG

De Algemene Verordening Gegevensbescherming gaat uit van beginselen waar elke verwerking van persoonsgegevens aan moet voldoen. Deze beginselen zijn de grondslag van dit privacybeleid.

Rechtmatigheid, behoorlijkheid en transparantie

We verwerken alleen persoonsgegevens voor gerechtvaardigde doeleinden. Dit betekent dat de verwerking noodzakelijk moet zijn met het oog op de grondslagen die genoemd worden in de AVG. Deze verwerkingen moeten vervolgens netjes en verantwoord gebeuren. We moeten transparant zijn over de verwerkingen die we uitvoeren. Dit betekend dat we betrokkenen actief informeren. We verwerken geen persoonsgegevens zonder dat ook maar iemand daarvan weet heeft.

Doeleinden

We verzamelen en verwerken alleen persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Wanneer we de gegevens later voor een ander doel gebruiken, dan moet dat nieuwe doel verenigbaar zijn met het oorspronkelijke verzameldoel. Dit doen we op basis van het beginsel “Eenmalige verstrekking, meervoudig gebruik”.

Dataminimalisatie

Wanneer we persoonsgegevens verwerken dan moeten zij voor het doel toereikend en ter zake dienend zijn. We verwerken niet meer persoonsgegevens dan noodzakelijk voor het doel. Met andere woorden, er mogen gelet op het doel, niet te veel, maar ook niet te weinig gegevens worden verwerkt voor het doel. Wanneer u namelijk te weinig gegevens verwerkt, dan kan er ten onrechte een onvolledig beeld ontstaan van de betrokkene.

Juistheid

We nemen alle redelijke maatregelen om ervoor te zorgen dat de gegevens correct en actueel zijn. Gegevens die dat niet (meer) zijn, wissen of corrigeren we.

Opslagbeperking

We bewaren persoonsgegevens niet langer dan noodzaken voor et doel van de verwerking. Hiervoor volgen we geldende regelgeving zoals de Archiefwet. Wanneer de gegevens niet langer noodzakelijk zijn, dan moeten zij worden vernietigd of gewist.

Integriteit en vertrouwelijkheid

We beschermen persoonsgegevens zo goed mogelijk tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Voor al de bovenstaande beginselen geldt dat wij verantwoordelijk zijn voor de naleving en dat we kunnen aantonen dat de gegevensverwerking in lijn is met de beginselen (de verantwoordingsplicht).

4. Uitgangspunten

Het privacybeleid gaat uit van een aantal uitgangspunten en kernwaarden van de gemeente Meppel. Deze zaken zijn in onderstaand hoofdstuk beschreven. Zo mogelijk is er een concreet handelingsperspectief of maatregel beschreven zodat het beleid toetsbaar en meetbaar is.

Het betreft de volgende uitgangspunten en kernwaarden:

A. We zetten de bedoeling van de vraagstukken centraal bij onze verwerkingen.
B. We leggen eigenaarschap vast bij onze verwerkingen en verantwoorden ons over waarom we persoonsgegevens verwerken
C. Wendbaar, flexibel en slagvaardig werken betekend dat de basis op orde moet zijn.
D. Juiste grondslag

A We zetten de bedoeling centraal

De gemeente Meppel wil doen wat nodig is en helpt, in plaats van alleen doen wat hoort. Dit terwijl privacy en digitale rechten worden beschermd. Dat is een voorwaarde voor wederkerig vertrouwen. Het gaat immers om de betekenis van wat de gemeente doet in het leven van de inwoner. We doen niets met persoonsgegevens wat we zelf niet snappen of niet kunnen uitleggen. Voor ons handelen betekent dat het volgende.

Handelen vanuit de geest van de wet

Onze taken zijn in beweging en we hebben een grote veranderopgave. De wettelijke regels zijn daar (nog) niet op toegerust. En dat vraagt soms dat we op de rand of buiten de kaders van de regels treden. Dat doen we risico georiënteerd, met inachtneming van ons moreel kompas en we maken het transparant. We kunnen het uitleggen en er verantwoording over afleggen. Dat vinden wij horen bij een betrouwbare overheid. Daarbij nemen we onze verantwoordelijkheid: we zetten de bedoeling centraal, zijn transparant en we doen het veilig. Dat geldt zowel voor het bestuur, de directie, teammanagers als voor individuele medewerkers.

B Betrouwbaar partnerschap

Van de gemeente mag betrouwbaar partnerschap worden verlangd. Een goede borging van privacy is daar onderdeel van. De basis op orde is niet alleen een randvoorwaarde, maar ook hoe wij vinden dat het hoort. Een goed ingericht gegevensbeheer levert meerwaarde op, bijvoorbeeld voor de continuïteit als er iets mis gaat (zoals een hack of ransomware), voor onze bedrijfsvoering (terugvindbaarheid, archivering en fysieke archiefruimte) en het vertrouwen dat onze inwoners en medewerkers in ons kunnen stellen.

Register van verwerkingen

We zijn verantwoordelijk voor het aanleggen van een register van alle verwerkingen die we uitvoeren. Het bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- de doelen van de verwerking;
- een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- een beschrijving van de ontvangers van de persoonsgegevens;
- een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie indien van toepassing;
- de termijnen waarin de verschillende persoonsgegevens moeten worden gewist.

De verantwoordelijkheid voor de inhoud, volledigheid en betrouwbaarheid van het register van verwerkingen ligt bij de teammanagers. De organisatie is verantwoordelijk voor het naleven van de beginselen van de AVG en moet de nalevingspraktijken van de organisatie kunnen aantonen. Door verantwoordelijkheden toe te kennen borgen en beheren we het register en implementeren we privacy in de reguliere bedrijfsvoering.

DPIA
We brengen privacy risico's vooraf in kaart en treffen zo beperkende maatregelen. We voeren op al onze verwerkingen met een hoog risico een risicoanalyse uit. We brengen risico's voor betrokkenen in kaart met gebruik van een DPIA. Het instrument is een middel om naleving van de privacyregelgeving te verbeteren. We gebruiken de uitkomsten van een DPIA voor het bepalen van de passende maatregelen. Zo kunnen we aantonen dat we de privacyregelgeving naleven.

Verwerkers
We hebben inzicht in onze verwerkers en hebben met alle verwerkers een verwerkersovereenkomst afgesloten. We gebruiken de standaard verwerkersovereenkomst van de VNG. Hierin zijn uniforme afspraken gemaakt over het verwerken van persoonsgegevens. Deze standaard is ontwikkeld door én voor gemeenten, in overleg met landelijke leveranciers.

Datalek
We houden een register bij van beveiligingsincidenten en datalekken. We hebben een procedure datalekken vastgesteld. Met deze procedure stellen we vast of een incident een datalek is dat gemeld moet worden aan de Autoriteit Persoonsgegevens (AP) en betrokken personen. Elk datalek moet intern geregistreerd worden. Verantwoordelijkheid voor het bijhouden van het register is belegd bij de privacy officer (PO). De PO overlegt indien noodzakelijk met de FG. Indien een datalek gemeld moet worden bij de AP dan dient het directieteam geïnformeerd te worden.

We maken allemaal fouten en iedereen mag fouten maken. We stimuleren onze medewerkers om te leren en bij een datalek lossen we het met elkaar op, maar het is niet vrijblijvend.

Rechten van betrokkenen
We houden rekening met de rechten van betrokkenen. Het beroepen op sommige rechten ligt meer voor de hand dan op andere rechten. Betrokkenen doen voornamelijk een beroep op inzage.

Voor de uitoefening van de rechten van betrokkenen is een protocol opgesteld. Dit protocol is voornamelijk bedoelt om vorm te geven aan het proces rondom het recht op inzage. Met dit protocol wordt een gestandaardiseerde werkwijze vastgelegd voor het uitvoeren van een verzoek van een betrokkene om gebruik te maken van één van zijn rechten conform de AVG. Verantwoordelijkheid voor dit protocol is belegd bij de Privacy Officer (PO). De PO overlegt indien noodzakelijk met de Functionaris Gegevensbescherming (FG).

Niet elk verzoek tot informatie moet opgevat worden als gebruik maken van bijvoorbeeld het recht op inzage. Daarnaast moet niet elke wijziging in contactgegevens gezien worden als een rectificatieverzoek. Indien dergelijke verzoeken informeel afgehandeld kunnen worden dan heeft dat de voorkeur. Het invulling geven aan de verschillende rechten van betrokkenen is bijna altijd maatwerk. De verzoeken dienen hierdoor ook specifiek te zijn en met redenen omkleed. Indien een betrokkene wil dat de gemeente gegevens verwijderd dan dient dit verzoek gemotiveerd zijn.

C Samen flexibel aan de slag

We verwachten van onze medewerkers een ontwikkelmindset en lerende houding, andere wegen een kans geven. De privacywetgeving geeft ons de kans om te kijken of het werkt en of het deugd. Hoewel het beperkingen oplegt dwingt het ons om na te denken of wat we doen deugd. En als het niet deugd andere wegen een kans te geven zodat het wel werkt. We zorgen dat betrokkene regie houdt op zijn gegevens. Dit doen we door te informeren wanneer, hoe, waarom en met wie we persoonsgegevens verwerken.

Bewustwording

Van onze medewerkers wordt verwacht de privacywetten en dit beleid naleven. Dit is in het belang van onze organisatie zelf én van degenen wiens gegevens verwerkt worden.

Om het onderwerp levend te houden wordt er jaarlijks een online cursus gegeven waar iedereen aan kan deelnemen. Daarnaast wordt er regelmatig op intranet en via andere kanalen aandacht geschonken aan informatiebeveiliging en privacy. Voorbeeld van onderwerpen:

- Hoe herken ik een datalek? bekendheid geven aan procedure melden datalek;
- verwerkersovereenkomsten actualiseren/AVG-proof maken;
- bewaar- c.q. vernietigingstermijnen. Vaststelling en naleving daarvan;
- inzagerecht betrokkene. Bekendheid aan geven, binnen én buiten de gemeentelijke organisatie.

Denkbaar is dat deze extra aandacht ook resulteert in aanpassing van dit beleid. Er zullen zich datalekken voordoen. Er kunnen fouten worden gemaakt in de verwerking van persoonsgegevens. Door de – op basis van dit beleid gegenereerde – extra aandacht voor dit onderwerp, wordt echter de kans op het maken van fouten verkleind.

Regie over eigen gegevens

We vinden de regie die Betrokkenen hebben op hun gegevens (‘informationele zelfbeschikking’) een belangrijk uitgangspunt. Daarvoor is (onder meer) informatie nodig en zijn we transparant waar dat kan.

De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Dit doen we bij de aanvang van een nieuwe verwerking. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop we met persoonsgegevens om gaan.

De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt. Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

We informeren betrokkenen als we persoonsgegevens verder verwerken dan waarvoor we de gegevens hebben gekregen. Dit doen we op basis van het beginsel “Eenmalige verstrekking, meervoudig gebruik”.

Als we persoonsgegevens van betrokkenen (moeten) delen bespreken we dat met hen. Maar in sommige situaties (bijvoorbeeld in het zorg- en veiligheidsdomein), kan het nodig zijn over betrokkenen te praten. We maken dan een expliciete afweging, die we vastleggen.

Op onze website staat een privacy verklaring. Met deze verklaring laat de gemeente Meppel zien op welke manier wij dagelijks omgaan met persoonsgegevens en privacy. En op welke wijze wij de privacy waarborgen, beschermen en handhaven. Per domein zijn afzonderlijke privacy verklaringen opgenomen. Hierin geven we weer wat het doel van de verwerking is en welke persoonsgegevens we daarvoor verwerken.

D Juiste grondslag

Voor het verwerken van persoonsgegevens moet aan het beginsel grondslag en doelbinding uit de AVG voldaan zijn. We starten pas met een verwerking als deze bekend zijn.

De AVG geeft zes grondslagen, dit zijn: Toestemming, Wettelijke verplichting, Overeenkomst, taak van Algemeen belang of een taak in het kader van de uitoefening van Openbaar gezag, Vitaal belang en Gerechtvaardigd belang. Elke grondslag heeft zijn eigen voorwaarden. We verwerken gegevens op basis van de grondslagen die bij onze rol als gemeente passen. Dat wil zeggen de grondslagen Wettelijke verplichting, taak van Algemeen belang of in het kader van een taak van Openbaar gezag. Wanneer we niet handelen als gemeente maar als bijvoorbeeld werkgever maken we gebruik van Gerechtvaardigd belang of Overeenkomst.

Wanneer we werkzaamheden uitvoeren vanuit onze publiekrechtelijke taak gebruiken we de grondslag Toestemming niet. Om deze grondslag te gebruiken met de toestemming vrij gegeven zijn. In onze rol als gemeente is er vaak een afhankelijkheidspositie ten opzichte van de inwoner. Deze heeft ons immers nodig. De toestemming kan in deze gevallen (volgens de Autoriteit Persoonsgegevens) niet vrij zijn.

Het is daarnaast in nagenoeg alle gevallen ook niet noodzakelijk om een betrokkene te vragen om toestemming voor de verwerking van persoonsgegevens. De grondslag taak van Algemeen belang of een taak in het kader van de uitoefening van Openbaar gezag is de juiste grondslag voor de uitvoering van een publiekrechtelijke taak die vastgelegd is in een wet. Tot slot moet toestemming als grondslag voor de verwerking van persoonsgegevens niet worden verward met andere betekenissen. Denk aan toestemming voor het instemmen met een voorgesteld behandelplan of een inwoner die toestemming geeft voor het digitaal communiceren met de overheid.

Als we gebruik maken van de grondslag Toestemming communiceren we duidelijk om welke verwerking het gaat en welke persoonsgegevens we gebruiken. Zodat de Toestemming vrij en op informatie gebaseerd is.

Bij de uitvoering van de AVG moet de sectorale wetgeving in acht worden genomen. Zo staat de AVG bijvoorbeeld niet op zichzelf in het sociaal domein, de AVG moet in relatie tot de specifieke wetgeving (Wmo, Participatiewet, Jeugdwet) binnen het sociaal domein worden gezien.

5 Governance

Het Privacybeleid staat niet op zichzelf en maakt onderdeel uit van een reeks aan maatregelen om de bescherming van c.q. de verwerking van persoonsgegevens binnen en door de gemeentelijke organisatie te optimaliseren. Het is een inherent onderdeel van ieders functie/van ieders dagelijks handelen. Tegelijkertijd is de bescherming van persoonsgegevens niet de core business van de meeste medewerkers. Er zijn daarom medewerkers die advies geven over en toezicht houden op de bescherming van persoonsgegevens binnen de organisatie.

5.1 Het bestuur

Het college van B&W stelt het privacybeleid vast en delegeert de uitvoering hiervan aan het directie team. Binnen het college valt de bescherming van persoonsgegevens onder de portefeuille organisatieontwikkeling & bedrijfsvoering. Het college informeert de Raad.

5.2 Directie team

De bescherming van persoonsgegevens is een aspect van de bedrijfsvoering, de bescherming van persoonsgegevens valt daarom onder de verantwoordelijkheid van het management. Het management zorgt er voor dat:

- De organisatie in staat is om de gedelegeerde verantwoordelijkheden te dragen;
- De controle op de het privacybeleid binnen de organisatie is gewaarborgd.

5.3 Teammanagers

Teammanagers zijn inhoudelijk verantwoordelijk voor naleving van wet- en regelgeving voor processen die binnen een bepaalt team vallen. Het gaat hier zowel om wet- en regelgeving die specifiek voor een bepaalt proces van toepassing zijn, zoals de Wmo voor het sociaal domein. Daarnaast is de betreffende teammanager ook verantwoordelijk voor naleving van de AVG voor de processen die binnen het team vallen.

De PO is procesverantwoordelijk voor het bijhouden van het register van verwerkingen. Wanneer nieuwe verwerkingen plaatsvinden of wijzigen binnen de gemeente dient de PO deze op te nemen in het register. De teammanagers zijn inhoudelijk verantwoordelijke voor de betreffende verwerkingen.

5.4 Functionaris Gegevensbescherming

De gemeente heeft een FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van het AP. Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de teams overneemt. De teams hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het gebied van privacy.

5.5 Privacy officer

Voor medewerkers én voor bestuurders is de privacy officer het dagelijkse aanspreekpunt bij vragen over de bescherming van persoonsgegevens voor zover deze niet binnen het domein van de coördinator informatiebeveiliging vallen. Ook ondersteunt de PO teams bij het opstellen van verwerkersovereenkomsten, het waar nodig mede-implementeren van adviezen van de FG, het opstellen van modellen, zoals een model-toestemmingsbrief. De PO vormt samen met de FG en de CISO het meldpunt datalekken. De PO vervangt de FG bij afwezigheid.

Zoals aangegeven, heeft de FG adviserende én toezichthoudende taken. Het gelijktijdig uitoefenen van beide taken kan spanningen geven. Wanneer dergelijke spanningen voorzienbaar én onwenselijk zijn, kan de PO de beantwoording van een concrete adviesvraag van de FG overnemen.

5.6 Chief Information Security Officer (CISO)

De CISO stelt het informatiebeveiligingsbeleid en de informatiebeveiligingsplanning op. Hij initieert/voert risicoanalyses uit en onderzoekt kwetsbaarheden of laat dit doen. Hij handelt informatiebeveiligingsincidenten af en coördineert bij grote beveiligingsincidenten. Hij stimuleert de bewustwording binnen en het bewustzijn van de organisatie over informatieveiligheid en risico's. Hij vormt samen met de FG en de PO het meldpunt datalekken.

De CISO adviseert gevraagd en ongevraagd het college, de directie en het lijnmanagement over risico's en te nemen maatregelen.

5.7 Themabijeenkomst Teammanagersoverleg

Het teammanagersoverleg wordt gevormd door het DT de teammanagers, de CISO, de FG en PO. Tijdens dit overleg worden respectievelijk domein overstijgende onderwerpen op de gebieden informatiebeveiliging en privacy besproken. Uitgangspunten uit dit overleg kunnen als advies dienen aan de verwerkingsverantwoordelijken.