Privacybeleid gemeente Meppel

Gemeente Meppel

Inhoudsopgave

1. Inleiding

De gemeente werkt met (Persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke (wettelijke) taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

1.1 Doelstelling

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. Wij zijn ons hiervan bewust en willen daarom met dit beleid aangeven hoe wij in algemene zin invulling geven aan nationale, Europese wet- en regelgeving en sectorspecifieke wetgeving, zoals de participatiewet en WMO, op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG) en Wet politiegegevens (hierna te noemen: Wpg).

De gemeente heeft BOA’s in dienst en zij verwerken gegevens die onder de AVG of onder de Wet Politiegegevens (Wpg) vallen. De Wpg is van toepassing op gegevensverwerkingen door BOA's in het kader van hun opsporingstaak. Hierbij gaat het om de opsporing van strafbare feiten. Dit privacy beleid is ook van toepassing op die gegevensverwerkingen. Daarnaast heeft de gemeente beleid en samenhangende procedures ingeregeld m.b.t. toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht.

Geldigheidsduur

Dit beleid is vastgesteld op 27 februari 2024 door het college van B&W. Het beleid wordt tenminste een keer per vier jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld in geval van grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA’s, o.i.d.) kan het college besluiten tot een tussentijdse herziening.

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

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.

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 we transparant in onze communicatie. We leggen eigenaarschap vast bij onze verwerkingen.

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.

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).

1.2 Achtergrond van het beleid

Privacy vraagt niet alleen om een heldere bestuurlijke visie op privacy maar ook om duidelijke beleidskaders. Privacywetgeving, waaronder de AVG en Wpg, biedt niet voor ieder vraagstuk een pasklaar antwoord maar schept juist ruimte door regels in de vorm van principes te formuleren waaraan 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.

1.3 Context en reikwijdte

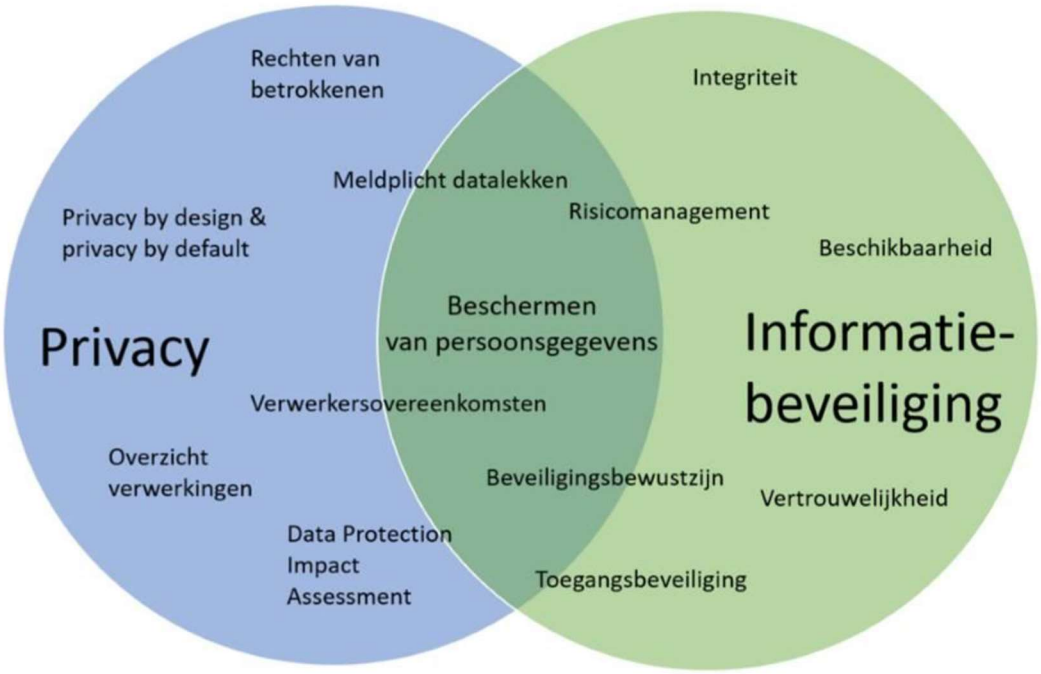
De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacy beleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente, waaronder:

1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

Dit privacy beleid bevat de domein overstijgende richtlijnen over hoe de bescherming van persoonsgegevens binnen de gemeentelijke organisatie wordt vormgegeven en georganiseerd. Het richt zich op eenieder 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 privacy beleid hangt samen met het Informatiebeveiligingsbeleid, waarbij de beleidsvelden samenkomen rond de beveiliging van persoonsgegevens. Deze relatie is visueel als volgt:



Figuur 1: Privacy en Informatiebeveiliging

De AVG en Wpg eisen 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.

2. Uitgangspunten

Het privacy beleid 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:

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

2.1 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.

2.1.1 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.

2.2 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 misgaat (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.

2.2.1 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.

2.2.2 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. Daarnaast informeert de PO altijd het DT bij een datalek dat hij meldt bij de AP.

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.

2.2.3 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.

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.

2.3 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 deugt. Hoewel het beperkingen oplegt dwingt het ons om na te denken of wat we doen deugt. En als het niet deugt 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.

2.3.1 Bewustwording

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

Om het onderwerp levend te houden maken we gebruik van micro vragen via email. Medewerkers moeten vragen beantwoorden over informatiebeveiliging en privacy. Daarnaast wordt er regelmatig op intranet en via andere kanalen aandacht geschonken aan informatiebeveiliging en privacy. Voorbeelden 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, verlaagt het risico op nadelige effecten voor onze inwoners.

2.3.2 Regie over de 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 privacyverklaring. 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.

2.4 Juiste grondslag

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

De AVG geeft zes grondslagen, dit zijn:

1. We hebben toestemming van de persoon om wie het gaat;
2. Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren;
3. Het is noodzakelijk om gegevens te verwerken omdat we dit wettelijk verplicht zijn;
4. Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen;
5. Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen;
6. Het is noodzakelijk om gegevens te verwerken om ons gerechtvaardigde belang te behartigen.

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.

3. Beginselen

De wetgever heeft een aantal beginselen opgenomen voor de verwerking van persoonsgegevens. De gemeente onderschrijft deze beginstelen en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes. Dit hoofdstuk geeft aan hoe we hier in Meppel invulling aan geven.

3.1 Rechtmatige grondslag

Persoonsgegevens worden door de gemeente slechts in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze verwerkt. Dit betekent onder meer dat verwerkingen slechts plaatsvinden als hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

3.2 Welbepaalde doeleinden

De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de gemeente alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De gemeente ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken of door het anonimiseren of aggregeren van gegevens.

3.3 Verdere verwerking

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor deze persoonsgegevens in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

3.4 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 namelijk te weinig gegevens worden verwerkt, dan kan er ten onrechte een onvolledig beeld ontstaan van de betrokkene.

3.5 Juiste en actuele gegevens

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.

3.6 Gegevens worden op tijd vernietigd

De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.
Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid.

Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

3.7 Integriteit en vertrouwelijkheid

De gemeente neemt passende technische en organisatorische maatregelen om de Persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht de gemeente om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

3.8 Privacy by Default en Privacy by Design

De gemeente houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt Privacy by Design (PbD) genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij geldt Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

3.9 Toegang tot gegevens

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de gemeente geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

3.10 Inbreuk in verband met persoonsgegevens

Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet altijd gemeld worden aan de Privacy Officer. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de procedure melden datalek. De gemeente registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan.
De Privacy Officer bepaalt, in overleg met de FG, het risico van het datalek en meldt dit, indien noodzakelijk bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen.

3.11 Samenwerking

De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.
Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat minimaal gelijk is aan dat van de gemeente.

3.12 Doorgifte buiten de EER

Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving, een SCC, een adequaatsheidbesluit en dit privacy beleid.

3.13 Transparantie

De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

3.14 Rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG en paragraaf 4 van de Wpg uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de procedure rechten van betrokkenen.

3.15 Geschillenbeslechting

Een betrokkene met een vraag, mededeling of klacht over het gebruik van persoonsgegevens door de gemeente kan contact opnemen via 140522 of postbus@meppel.nl.
Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website. Personen hebben het recht om na afhandeling van een klacht hiertegen verweer te voeren bij de FG voor zover het verweer gericht is op de naleving van privacywetgeving en/of het privacy beleid van de gemeente. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.
Vragen worden zo snel mogelijk, maar uiterlijk binnen vier weken afgehandeld. Indien een vraag niet tot tevredenheid is afgehandeld, hebben betrokkenen het recht zich opnieuw te wenden tot de gemeente via 140522 of postbus@meppel.nl.

3.16 Verantwoording

Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

3.17 Verwerkingsregister

- We zijn verantwoordelijk voor het bijhouden 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 Wpg 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.

3.18 DPIA

Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De gemeente voert in dat geval een DPIA uit. Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd.
Nadere regels ten aanzien van het uitvoeren, vaststellen en afhandelen van DPIA's zijn opgenomen in de procedure uitvoeren DPIA.

3.19 Functionaris gegevensbescherming (FG)

De gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere en strafrechtelijke persoonsgegevens. De gemeente is daarom verplicht een FG aan te stellen. De FG is de onafhankelijke interne toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan de gemeenteraad en het College van B&W van zijn werkzaamheden, bevindingen en aanbevelingen.

3.20 PDCA Cyclus

De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

3.21 Bewustwording

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

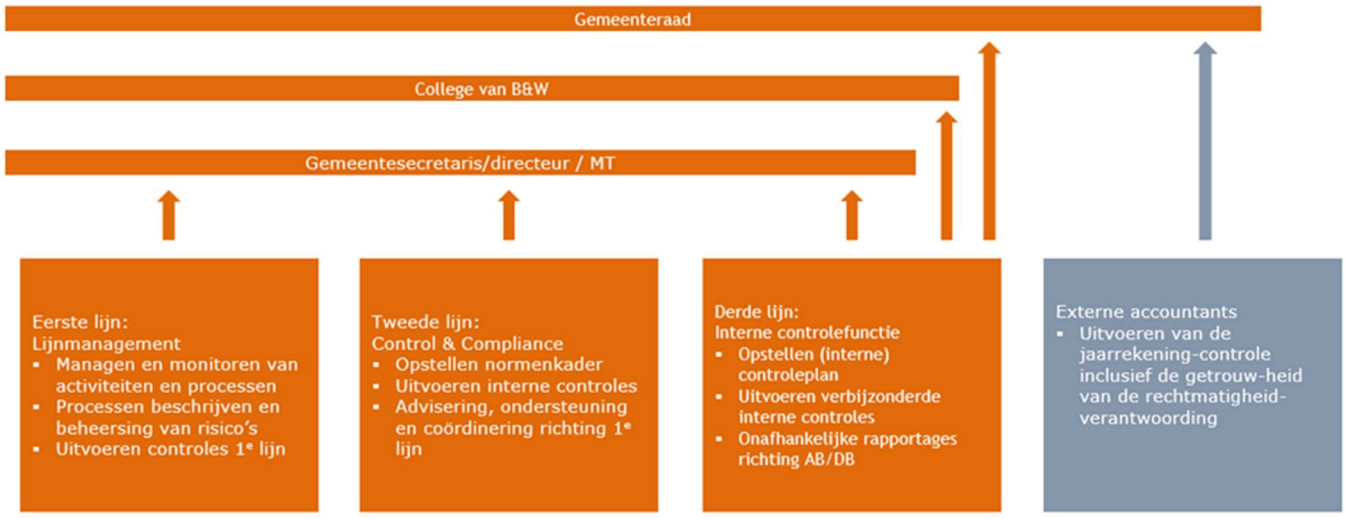
3.22 Audits

De Wpg kent een auditverplichting. Eén keer in de 4 jaar is een externe audit verplicht. We laten dan controleren in hoeverre we voldoen aan de eisen die de wet stelt aan de verwerking van politiegegevens. In 2022 heeft de gemeente Meppel aan deze verplichting voldaan. De rapportage met bevindingen delen we met de Autoritieit Persoonsgegeven (AP). In de jaren dat er geen externe audit plaatsvindt, voert de gemeente zelf een interne audit uit. De rapportage deelt de auditor met het College van B&W. De audit wordt uitgevoerd door een medewerker van de gemeente die geautoriseerd is voor deze rol.

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

4. Rollen en taken

Het privacy beleid 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.



Figuur 2: Rollen en taken

4.1 Het college van B&W

Het College is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. Het College heeft de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente;
- Stelt het privacy beleid vast;
- Geeft sturing aan privacy beleidsvoering en legt rekenschap af over privacy beleidsvoering aan de FG;
- Evalueert de toepassing en werking van het privacy beleid op basis van de rapportage van de FG;
- Bevordert duurzame privacy cultuur.

4.2 Directieteam

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 ervoor dat:

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

4.3 Teammanagers

Teammanagers zijn eigenaar van de verwerking en daarmee 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 en Wpg voor de processen die binnen het team vallen.

4.4 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.

4.5 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. 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. 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.

4.7 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.

4.8 Informatiemanager

De Informatiemanager ondersteunt de teams bij het bepalen van de benodigde inrichting van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze/ in welk systeem verwerkt kan/ moet worden).

4.9 Functioneel Beheerder

De Functioneel Beheerder draagt zorg voor functionele inrichting van informatiesystemen in overeenstemming met de wensen en eisen van de eigenaar van de verwerking. Daarbij houden ze rekening met de adviezen vanuit de informatiemanager, CISO en de FG.

Daarnaast kan de Functioneel Beheerder gevraagd en ongevraagd adviseren over aanpassingen aan de inrichting van informatiesystemen vanuit nieuwe/gewijzigde wet-/regelgeving en signaleert mogelijke datalekken.

4.10 Medewerkers gemeente Meppel

Onze medewerkers krijgen, zien en werken met veel gevoelige informatie. Zij gaan zorgvuldig om met de (persoons)gegevens waarmee zij werken en zorgen er tijdig voor dat inbreuk van de gegevens (datalekken) gemeld wordt bij de PO.

4.11 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.

Bijlage 1: Begrippen

Algemene Verordening Gegevensbescherming (AVG)

De AVG is Europese privacywet. Deze wet sluit beter aan op het digitale tijdperk waarin we leven. De wet geeft burgers meer rechten en de gemeente meer verantwoordelijkheid om zorgvuldig met (digitale) persoonsgegevens om te gaan.

Betrokkene

Voornamelijk 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.

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 beschikbaarheid, gegevens zijn niet beschikbaar;
- Inbreuk op de integriteit, gegevens zijn niet correct;
- Inbreuk op de vertrouwelijkheid, gegevens kunnen worden ingezien door niet geautoriseerde personen.

Een datalek kan, afhankelijk van de omstandigheden, in meer dan één van deze drie categorieën vallen.

Data Protection Impact Assessment (DPIA)

Een DPIA (of gegevensbeschermingseffectbeoordeling) 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).

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.

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 alleen of samen met anderen 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.

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).

Wet politiegegevens (WPG)

De Wet politiegegevens is een wet die de rechten en de plichten van de politie zelf, maar ook die van de burger regelt, voor wat betreft het verwerken van politiegegevens. Politiegegevens zijn persoonsgegevens die in het kader van de politietaak worden verwerkt. Naast de politie moeten ook andere organisaties zich aan de Wpg houden: de bijzondere opsporingsdiensten (BOD) en de buitengewoon opsporingsambtenaren (boa's). De gemeente heeft BOA’s in dienst en zij verwerken gegevens onder de AVG of onder de Wpg.

Duurzaamheid in Gemeente Meppel

Gemeente Meppel staat voor duurzaamheid. Dit document is ontworpen voor online gebruik.
Wil je het document toch printen? Print dan in zwart-wit en minimale printkwaliteit.

Kijk voor meer informatie over duurzaamheid in Gemeente Meppel op www.meppel.nl/duurzaam.