Strategisch Privacybeleid

Gemeente Meierijstad 2020 – 2023

COLOFON

Naam document	Strategisch privacybeleid 2020-2023
Versie	1.0
Datum	18-2-2020
Status	Definitief
Zaaknummer	1948307174
Documentnummer	1948966771

Auteur(s)	Ed Gruter

Goedgekeurd door:

Naam	**Rol**

Wijzigingen:

Versie	**Datum**	**Omschrijving wijzigingen**
0.1	11-12-2019	Conceptversie ter review.
0.2	23-1-2020	Reviewopmerkingen Functionaris Gegevensbescherming en Gemeentesecretaris verwerkt.
0.3	28-1-2020	Reviewopmerkingen Atelier Informatiestrategie verwerkt.
0.4	12-2-2020	Opmerkingen Directeur Bedrijfsvoering verwerkt.
1.0	18-2-2020	Definitieve versie

Inhoudsopgave

1 INLEIDING

1.1 ALGEMEEN

We leven in een informatiesamenleving. We zijn en worden in steeds grotere mate afhankelijk van betrouwbare informatiesystemen en data. Die afhankelijkheid wordt veroorzaakt door diverse ontwikkelingen die kansen bieden om de bedrijfsvoering en dienstverlening effectiever en efficiënter in te richten en te innoveren waardoor voldaan kan worden aan de (veranderende) behoeften en wensen om ons heen, bij onze (samenwerkings)partners, onze inwoners, ondernemers en onszelf.

Zo fungeren wij als gemeente in een keten. Binnen de gemeente Meierijstad wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Wij ontvangen en delen data met andere organisaties.
Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van de gemeentelijke wettelijke taken. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat. Voor de keten is het essentieel dat betrouwbare data en informatiesystemen worden gebruikt om inwoners en ondernemers te voorzien van producten en diensten.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. Het college van B&W is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Het college van B&W geeft middels dit beleid op strategisch niveau duidelijk richting aan privacy en laat daarmee zien dat zij de privacy van inwoners en medewerkers waarborgt, beschermt en handhaaft. De organisatie betracht daarbij grote zorgvuldigheid in het doorlopend manoeuvreren tussen het werkbaar houden van de werkzaamheden en het correct toepassen van de wet- en regelgeving. Dit beleid is kader stellend en beschrijft ook de wijze waarop de verantwoordelijkheden zijn belegd en die van toepassing zijn op de ambtelijke en bestuurlijke organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente.

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket aan maatregelen om de betrouwbaarheid van de informatievoorziening te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid), vertrouwelijkheid en controleerbaarheid van persoonsgegevens en andere informatie. Dit Privacybeleid is samen met het Informatiebeveiligingsbeleid gericht op het waarborgen van deze informatieveiligheid.

Hoofdstuk 1 beschrijft de kaders en geeft aan welke informatie is gebruikt om het beleid te formuleren. De hoofdstukken 2 en 3 beschrijven het beleid en lichten de taken en verantwoordelijkheden binnen het beleidsgebied privacy toe.

1.2 DEFINITIES

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geidentificeerd, 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.

Betrokkene
Degene op wie de persoonsgegevens betrekking hebben, tevens eigenaar van de persoonsgegevens.

Verwerkingsverantwoordelijke
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lid statelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

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

Verwerking
Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

1.3 HET BELANG VAN PRIVACY EN PRIVACYBESCHERMING

Privacy is de persoonlijke levenssfeer die onszelf en ons handelen, eigenschappen en informatie onderscheidt van anderen. Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda.

Gemeenten hebben de verantwoordelijkheid voor persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn, waarbij ze vanuit privacy perspectief een van de meest complexe organisaties zijn die we kennen. Gemeenten zijn verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Dat geldt onder andere voor taken op het gebied van basisadministraties, openbare orde en veiligheid en het sociaal domein. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van gemeenten.

Het beschermen van de privacy is complex en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van openbare veiligheid en nieuwe Europese wetgeving. De gemeente is zich hier van bewust en zorgt ervoor dat de privacy

van betrokkenen gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie en gebruikerscontrole.
Tenslotte gaat de gemeente op een transparante wijze om met de gegevens die ze verwerkt. Dit houdt in dat we aan betrokkenen duidelijk maken in welke gevallen we persoonsgegevens verwerken, hoe we dit doen en waarom.

1.4 DOEL PRIVACYBESCHERMING

Privacybescherming waarborgt dat de persoonsgegevens die de gemeente verwerkt, niet alleen organisatorisch en passend beveiligd zijn, maar dat de persoonsgegevens ook op de juiste wijze worden gebruikt, met in acht neming van eisen in de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

De AVG stelt regels vast betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens zoals noodzakelijkheid, doelbinding, proportionaliteit en subsidiariteit. Daarnaast beschermt deze verordening de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens.
Op een aantal punten laat de AVG ruimte voor nationale keuzes. Deze zijn uitgewerkt in de UAVG.

Privacybescherming zorgt ervoor dat wij onze missie, visie en (politieke) doelen kunnen realiseren, op een verantwoorde manier, waarbij risico's gemanaged worden.

1.5 WETTELIJKE KADERS

In artikel 10 van de Grondwet is het recht op privacy geregeld:
‘Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.’

Met de invoering van de AVG verscherpen de eisen waaraan verwerkingen van persoonsgegevens moeten voldoen. De AVG vraagt echter om meer dan enkel ordentelijk met persoonsgegevens omgaan.
De AVG vraagt om nieuw denken en handelen:

Persoonsgegevens zijn en blijven eigendom van de betrokkene.

Dankzij deze nieuwe wetgeving dringt gegevensbescherming en privacy door in alle processen binnen de gemeentelijke organisatie.

Dit privacybeleid is in lijn met het algemene beleid van de gemeente Meierijstad en de relevante lokale, regionale, nationale en Europese wet- en regelgeving. De gemeente is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden de volgende wettelijke kaders:

- Europese Verordening; de Algemene Verordening Gegevensbescherming (AVG) Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)

Naast de algemene wettelijke kaders spelen, naast de gemeentelijke visie, ook de volgende wetten en normen in het bijzonder een rol:

- Archiefwet (voor de bewaartermijnen van gegevens)
- Wet openbaarheid van bestuur (WOB)

- Visie op Meierijstad 2025
- Informatiebeleidsplan 2018-2022
- Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2020 – 2023
- A3 concernplan 2019
- Wet open overheid (WOO)
- Aanvullingen op dit algemene kader in sectorspecifieke wetten, zoals wetten op het terrein van het sociaal domein.

1.6 REIKWIJDTE VAN HET PRIVACYBELEID

Dit beleid is van toepassing op zowel het privaat- als publiekrechtelijk deel van de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente en wordt bij voorkeur ook toegepast in samenwerkingsverbanden die de gemeente aangaat.

Specifiek voor de verwerking van persoonsgegevens zijn de AVG, de UAVG en de daarop berustende bepalingen van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

1.7 OPBOUW STRATEGISCH PRIVACYBELEID

Het strategisch beleid bestaat uit de kaders die leidend zijn voor privacy. Deze zijn veelal gebaseerd op bestaande wet- en regelgeving en geven de principes die privacy en de betrouwbaarheid van de informatie(systemen) waarborgen. Het strategisch beleid vormt samen met een tactisch en operationeel plan één geheel, waarin de gehele set aan eisen en maatregelen ten behoeve van privacy is afgedekt.

In het tactische plan worden de kaders uitgewerkt en vertaald in een generieke set van maatregelen. In operationele plannen worden op het laagst mogelijke niveau de maatregelen verder uitgewerkt en vastgesteld door de verantwoordelijke.

2 PRIVACYBELEID

2.1 ORGANISATIE: GOVERNANCE

In het kader van de borging van Privacy en de AVG in de organisatie is onderstaande governance structuur vastgesteld. Hiermee wordt de samenhang en transparantie in het bestuur en toezicht gewaarborgd met het oog op een efficiënte en effectieve realisatie van de beleidsdoelstellingen.

Bestuurlijke verantwoordelijkheid

Het college van Burgemeester en Wethouders is bestuurlijk eindverantwoordelijk voor privacy en de verwerking van persoonsgegevens die onder verantwoordelijkheid van de gemeente Meierijstad worden uitgevoerd tenzij vanuit een specifieke wettelijke regeling de Burgemeester, de Heffingsambtenaar of Gemeenteraad verantwoordelijk is. Dit privacybeleid vloeit daaruit voort. Het college van B&W wordt geadviseerd door de Functionaris Gegevensbescherming.

Aansturing
De Gemeentesecretaris adviseert het college van B&W over het (privacy)beleid en over de mate waarin privacy een onderdeel is in het handelen van de bedrijfsvoering. Zij vormt met de Directie het directieteam dat verantwoordelijk is voor het vertalen van het strategische privacy beleid naar tactisch niveau. Het directieteam wordt daarbij geadviseerd door de Functionaris Gegevensbescherming en/of Privacy officer. Het directieteam zorgt daarbij dat op termijn alle processen, systemen en daarbij behorende middelen onder verantwoordelijkheid vallen van een Proceseigenaar.

Uitvoering
De Proceseigenaar is verantwoordelijk voor de borging van de AVG in de processen. Ter ondersteuning van deze verantwoordelijkheid wordt binnen het atelier of cluster van ateliers een privacy contactpersoon benoemd die belast is met de toepassing van de AVG in de processen. Afhankelijk van de grootte of complexiteit van processen in het atelier kunnen extra medewerkers ter ondersteuning van de Privacy contactpersoon worden toegevoegd. De privacy contactpersoon is eerste aanspreekpunt voor de medewerkers in het atelier betreffende AVG vragen en daarmee de schakel naar de Privacy officer.

Controle, verantwoording en toezicht.
De Autoriteit Persoonsgegevens (AP) is de Nederlandse gegevensbeschermingsautoriteit en het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens. De Autoriteit Persoonsgegevens kan uit eigen beweging een onderzoek doen naar de naleving van de privacywetgeving. Daarnaast kan de Autoriteit Persoonsgegevens op verzoek van belanghebbenden (zoals burgers of belangenorganisaties) een onderzoek instellen.

De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van B&W en directieteam over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG fungeert als contactpersoon tussen gemeente en AP en kan deze laatste ook rechtstreeks inschakelen.

De Privacy Officer (PO) werkt in opdracht van het College van B&W en Directieteam met als doel de borging van de AVG en UAVG in de gehele organisatie. De focus ligt hierbij op advies, toetsing en ondersteuning, zowel op strategische, tactische en operationele taken. De Privacy Officer geeft invulling aan de uitwerking van en rapportage over privacy beleidsonderwerpen en de AVG. De Privacy Officer is het eerste aanspreekpunt voor de privacy contactpersoon uit de ateliers.

Escalatie
De FG en PO beschikken niet over formele sanctiebevoegdheden. Bij constatering van ernstige gebreken in het toepassen van de privacywetgeving en/of het niet volgen van de privacy richtlijnen waarbij ernstige risico’s bestaan voor de organisatie of betrokkenen escaleert de FG direct naar het DT en college van B&W, de PO direct naar het DT.

In de bijlage zijn de taken en verantwoordelijkheden verder uitgewerkt. Deze bijlage moet hier als volledig ingelast worden beschouwd.

2.2 UITGANGSPUNTEN

De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van haar klanten. In de uitoefening van haar publiekrechtelijke taak houdt zij zich aan de wet en zoekt waar mogelijk de ruimte om de privacybelangen van zowel de burger als de doelstellingen van de gemeente naar beste inzicht te behartigen. De gemeente houdt zich hierbij aan de beginselen uit de AVG.

Het “Informatiebeleidsplan 2018-2022” beschrijft dan ook als een van de uitgangspunten:

> *“Betrouwbaarheid in dienstverlening en privacy is essentieel. Daarbij werken we vanuit de ‘bedoeling van de wet’. We organiseren maximale transparantie bij het verzamelen, gebruiken en verwijderen van gegevens van burgers, bedrijven en instellingen.”*

De gemeente naast het privacy beleid ook een privacy missie geformuleerd. Een missie is datgene dat de organisatie naar buiten wil uitdragen. Het geeft aan waarvoor de mensen uit de organisatie staan, wat hun identiteit en waarden zijn, welke gedragsregels gehanteerd worden.

Gedragsregels vinden hun oorsprong in de Fair Information Principles (FIP) en zijn internationaal erkende privacy principes over hoe om te gaan met persoonsgegevens. Zij vormen het fundament voor veel (inter)nationale privacywetten, regelgeving en verdragen, zo ook voor de AVG. De specifieke rechten en plichten zoals verwoord in de AVG vormen eigenlijk een uitwerking van de Fair Information Principles. De FIPs zijn dan ook de ruggengraat van de AVG en de basis van de beginselen van het privacy beleid.

2.3 BEGINSELEN

Rechtmatigheid, behoorlijkheid, transparantie

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. De gemeente is open over het feit dat we noodzakelijke persoonsgegevens verwerken en voor welke doeleinden. De betrokkene wordt helder geïnformeerd over zijn rechten, bijvoorbeeld via de website van de gemeente Meierijstad. Alleen indien de wet anders bepaalt wijkt de gemeente van deze informatieplicht af.

Grondslag en doelbinding

De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

Dataminimalisatie

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

Bewaartermijn

Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. Voor gemeenten gelden daarvoor de Archiefwet of andere wetten. Deze wetten regelen het beheren van archieven en documenten voor de lange termijn zodat ze beschikbaar komen voor iedereen die daar onderzoek in wil doen. De Archiefwet houdt

daarbij rekening met de privacy door zo nodig van persoonsgegevens de openbaarheid te beperken.

Integriteit en vertrouwelijkheid
De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Dit sluit aan bij het “Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2020-2023” van de gemeente Meierijstad wat is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). Gezamenlijk vormen deze maatregelen de technisch afdoende bescherming waar de privacywetgeving om vraagt.

Delen met derden
In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet en worden vastgelegd in een verwerkersovereenkomst.

Subsidiariteit
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

Proportionaliteit
De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met het in de verwerking te dienen doel.

Rechten van betrokkenen
De gemeente honoreert alle rechten van betrokkenen en heeft hiervoor processen en procedures ingericht.

2.4 NALEVING VAN HET BELEID

De naleving van het beleid krijgt vorm in reguliere werkzaamheden die op basis van een methodische aanpak alle organisatorische verplichtingen uit de AVG borgen. Via een Plan-Do-Check-Act cyclus wordt de continuïteit geborgd van opgeleverde producten en procedures. Een aantal onderwerpen wordt hier nader toegelicht.

Aantoonbaarheid
De AVG verplicht organisaties om aan te kunnen tonen dat aan de voorwaarden uit de wet wordt voldaan. Door middel van (deels) verplichte overzichten, registers en andere documenten wordt de bewijslast samengesteld en verzameld. Zo wordt er een register bijgehouden met alle verwerkingsactiviteiten van persoonsgegevens per proces, het verwerkingsregister.

Waar mogelijk maakt de gemeente gebruik van landelijke standaards en producten van de Vereniging Nederlandse Gemeenten (VNG) / Informatie Beveiligings Dienst (IBD). De gemeente is nauw betrokken bij de ontwikkeling van tools en hulpmiddelen via de VNG/IBD.

Bewustzijn privacy
Privacy is voor een groot deel afhankelijk van het menselijk handelen. Het beleid richt zich dan ook op het vergroten van de kennis van de AVG en het bewust omgaan met persoonsgegevens door de medewerkers. Hiervoor is een bewustwordingsprogramma opgesteld.

Meldplicht datalekken
Het gaat bij een datalek om situaties waarbij een onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden of kan plaatsvinden. Een datalek wordt intern en indien nodig bij de Autoriteit Persoonsgegevens en de betrokkene(n) gemeld. De gemeente voorziet in procedures voor registratie en afhandeling. Deze procedure bevat een vastgesteld proces van te doorlopen stappen om de eventuele schade of de kans hierop te beperken en de getroffen perso(o)n(en) te beschermen.
Alle datalekken worden geregistreerd in een datalek register.

Verwerkingsregister
Er is een register van verwerkingen welke inschrijvingen bevat van alle binnen de gemeente vastgestelde verwerkingen van persoonsgegevens. Bij de inschrijving worden in ieder geval de volgende gegevens vermeld:

a. de naam van de verwerking;
b. wie de verantwoordelijke is voor de verwerking;
c. het doel van de verwerking;
d. de groep van personen van wie persoonsgegevens worden verwerkt (betrokkenen);
e. de categorie persoonsgegevens die bij de verwerking worden gebruikt;
f. de ontvangers van de gegevens;
g. de rechtmatige grondslag voor de verwerking van de persoonsgegevens;
h. eventuele verstrekkingen aan andere landen buiten de Europese Economische Ruimte;
i. de verwijderingstermijnen die in acht genomen worden;

Privacy by default
De standaard instellingen in systemen zijn ingesteld om maximale privacy bescherming te borgen. Voor die producten of diensten waarbij betrokkenen zelf de mogelijkheid wordt geboden om persoonsgegevens te delen of af te staan worden de instellingen en functies van de producten of diensten standaard (by default) op de meest privacy vriendelijke stand gezet.

Privacy by design
Bij de aanschaf, ontwikkeling en inrichting van ICT infrastructuur en/of applicaties is het van belang om aan de voorkant van het (inkoop)proces de belangen en werkprocessen vanuit privacy-oogpunt te borgen. Door het borgen van de privacyaspecten aan het begin van het inkoop, ontwikkel- en inrichtingsproces wordt ervoor gezorgd dat problemen met privacy zo veel mogelijk worden beperkt. Privacy by designmaatregelen worden toegepast onder meer bij het afsluiten van verwerkersovereenkomsten, toegangsbeveiliging, encryptie, verwijderen van persoonsgegevens, dataminimalisatie.
Als uitgangspunt kiest de gemeente voor technische maatregelen om de privacy door ontwerp te waarborgen. Daar waar de technische mogelijkheden ontbreken of disproportioneel hoge kosten met zich meebrengen, zoekt de gemeente naar organisatorische en of procesmatige maatregelen als alternatief voor of als aanvulling op de technische maatregelen.

Verwerkers en verwerkersovereenkomst
Wanneer de gemeente een partij inschakelt om ten behoeve van de gemeente persoonsgegevens te verwerken kan deze partij worden beschouwd als verwerker. De gemeente schakelt enkel verwerkers in die afdoende garanties bieden met betrekking tot het toepassen van passende technische, procesmatige, communicatieve en organisatorische maatregelen. De afspraken omtrent de verwerking door de verwerker worden schriftelijk vastgelegd in een verwerkersovereenkomst en worden voordat de dienstverlening aanvangt en daarna periodiek of steekproefsgewijs getoetst.

Gegevensbeschermingseffectbeoordeling (DPIA)
100% informatieveiligheid bestaat niet. Het voldoende weerbaar zijn houdt de gemeentelijke organisatie open en verbonden met de (veranderende) behoeften en wensen van de maatschappij. Het maakt de organisatie flexibel. Risico's moeten voldoende beheerst worden, wat betekent dat een risico-gestuurde aanpak essentieel is.
Nieuwe en complexe bestaande verwerkingen worden onderworpen aan een (verplicht) Data Protection Impact Assessment (DPIA). De gemeente gebruikt dit instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen en om daarna maatregelen te kunnen nemen om de risico's te verkleinen. Door risico's inzichtelijk te hebben, kunnen afgewogen besluiten worden genomen om uitvoering te geven aan onze missie, visie en doelen.

Jaaragenda
Jaarlijks wordt een aantal onderwerpen benoemd die specifieke aandacht behoeven bijvoorbeeld als gevolg van gewijzigde of nieuwe wet- en regelgeving. Ook geeft de AP geeft richtlijnen over te toetsen aandachtsgebieden of onderdelen van de AVG. De activiteiten die hieruit voortvloeien worden opgenomen in de privacy jaaragenda.

2.5 DOEL 2020 - 2023

Met de definitie en uitvoering van dit privacy beleid beoogt de gemeente voor eind 2023 de volgende doelstellingen te hebben gerealiseerd:

1. De gemeente Meierijstad is een betrouwbare organisatie met betrekking tot dienstverlening en privacy met een maximale transparantie bij het verzamelen, gebruiken en verwijderen van gegevens van burgers, medewerkers, bedrijven en instellingen.
2. De rechten van betrokkenen worden gerespecteerd en conform de gestelde eisen uitgevoerd.
3. AVG en privacy zijn een integraal onderdeel van het reguliere bedrijfsproces en als zodanig geborgd via de governance, het strategisch, tactisch en operationeel beleid, overlegstructuren, organisatie (ateliers) en processen.
    a. Er is een privacy organisatie met FG en PO's die organisatie breed zorgdraagt voor advisering, toetsing en ondersteuning op strategisch, tactisch en operationeel niveau.
    b. Het register van verwerkingen is gekoppeld aan de processen en up-to-date.
    c. Binnen de ateliers zijn contactpunten die op operationeel niveau het aanspreekpunt zijn voor 1e-lijns privacy vraagstukken. De contactpunten (kunnen) worden bijgestaan door een aantal meer ervaren medewerkers. (functionerende 3-traps raket)
    d. Alle medewerkers hebben een minimale basiskennis van de privacy wetgeving en weten deze bewust toe te passen in hun dagelijks werk.

4. Gemeente Meierijstad voldoet aan de wettelijke verplichtingen voortvloeiend uit de AVG en kan dit op ieder moment met bewijs aantonen.
5. De status van de borging van de AVG wordt conform de Plan-Do-Check-Act cyclus onderhouden.

BIJAGE: TAKEN EN VERANTWOORDELIJKHEDEN

COLLEGE VAN BURGEMEESTER & WETHOUDERS

Het college van Burgemeester en Wethouders is eindverantwoordelijk voor privacy binnen de gemeente Meierijstad. Met het bekrachtigen van het beleid ten aanzien van privacy belegt het college van B&W de uitvoering en naleving hiervan bij het ambtelijk apparaat.

PORTEFEUILLEHOUDER PRIVACY

De wethouder met in de portefeuille het beleidsgebied privacy vertegenwoordigt daarmee het College van B&W. De wethouder heeft over dit gebied veelvuldig overleg met het directielid bij wie privacy belegd is.

DIRECTIETEAM

De gemeentesecretaris vormt samen met de directieleden het directieteam en is verantwoordelijk voor de vertaling en uitvoering van het privacybeleid naar de organisatie. De gemeentesecretaris adviseert het college van B&W. Het beleidsgebied privacy is belegd bij de directeur bedrijfsvoering. In de privacy organisatie fungeert de directeur bedrijfsvoering als opdrachtgever naar de Privacy officer. Het directieteam stelt kaders en geeft sturing ten aanzien van privacy op tactisch en operationeel niveau, evalueert beleidskaders en controleert of de uitvoering van de (U)AVG in de organisatie voldoende geborgd is.

FUNCTIONARIS GEGEVENSBESCHERMING

De Functionaris Gegevensbescherming (FG), is de wettelijke interne toezichthouder op de verwerking van persoonsgegevens binnen de organisatie. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de privacywetgeving. De wettelijke taken en bevoegdheden[1] van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG heeft in ieder geval de volgende verantwoordelijkheden:

- Informeren en adviseren van de gemeente en de verwerkers die namens de gemeente persoonsgegevens verwerken over hun verplichtingen volgens de AVG ;
- Toezien op naleving van AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming, op naleving van het gemeentelijke privacybeleid, toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- Adviseren en rapporteren met betrekking tot vraagstukken over de verwerking van persoonsgegevens, veiligheidsincidenten en Data Protection Impact Assessment (DPIA);
- Toezien op en adviseren over de afhandeling van (formele) verzoeken, vragen en klachten over het gebruik van persoonsgegevens, ondersteunen bij het opstellen van privacy normen en procedures, beleid, regelingen en/of gedragscodes;
- Afsluiten, beheren en actualiseren van verwerkersovereenkomsten;
- Rapporteert rechtstreeks aan het college van B&W en het Directieteam;

[1] De taken van de FG zijn vastgelegd in AVG-Art 39. In de praktijk is een deel van de uitvoering van deze taken uitbesteed aan de Privacy Officer. De wettelijke verantwoordelijkheid blijft echter bij de FG.

- Optreden als contactpunt met de Autoriteit Persoonsgegevens (AP), verzorgen van meldingen en intrekkingen van meldingen van datalekken bij de AP;

PRIVACY OFFICER

De Privacy Officer werkt in opdracht van het College van B&W en Directie met als doel de borging van de AVG en UAVG in de gemeentelijke organisatie en legt daarover verantwoording af. De privacy officer adviseert de organisatie over de toepassing daarvan bij informatieprocessen en systemen. De focus ligt hierbij naast de strategische ook op de tactische en operationele taken. Deze rol is gericht op coördinatie en ondersteuning van de uitvoering en de naleving van de privacy wetgeving door de procesbeheerders en medewerkers in algemene zin. De Privacy Officer adviseert over privacybescherming en over andere activiteiten ter bescherming van persoonsgegevens. De Privacy Officer heeft in ieder geval de volgende taken:

- Het beoordelen van de verwerking(en) van persoonsgegevens tegen de achtergrond van de kaders van de AVG. De Privacy Officer adviseert Leidinggevenden, Proceseigenaren en Contactpersonen bij wijzigingen in procesuitvoering en bedrijfsvoering en de uitvoering van een Data Protection Impact Assessment (DPIA);
- Als adviserend lid deelnemen aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens;
- Het uitleggen en uitdragen van de privacy-voorschriften uit de AVG en de daarmee verbonden sectorale wetgeving;
- De toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van privacy en de rapportage hierover;
- Het coördineren van de privacy-werkzaamheden van, in eerste instantie, de aan hem toegewezen werkprocessen dan wel verwerkingen met persoonsgegevens;
- Het in behandeling nemen en coördineren van datalek meldingen, verzoeken om inzage, correctie en beperking ten aanzien van (de verwerking van) persoonsgegevens;
- Adviseren en ondersteunen bij het besluitvormingsproces over, en het afsluiten van verwerkersovereenkomsten, convenanten en de vaststelling van reglementen; Bijdragen aan het privacy-bewustzijn.

PROCESEIGENAAR

De proceseigenaar is verantwoordelijk voor een of meer bedrijfsprocessen, zowel op tactisch als operationeel niveau. De proceseigenaar is daarmee ook eindverantwoordelijk voor de borging van de AVG binnen dat proces, het bijbehorende verwerkingsregister en wordt daarbij ondersteund door de contactpersoon privacy. De proceseigenaar rapporteert aan het directieteam over de door hen tactisch en operationeel uitgevoerde privacy activiteiten. Waar nodig wint de proceseigenaar informatie of advies in bij de FG of PO. Taken van de proceseigenaren in het kader van privacy zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen processen en werkateliers uitdragen van het privacybeleid en de daaraan gerelateerde procedures.
- Het vroegtijdig betrekken van FG of PO bij aanpassingen of nieuwe processen.
- Bespreking van privacy incidenten en de mogelijke gevolgen voor beleid en maatregelen.

CONTACTPERSOON PRIVACY

De rol contactpersoon privacy wordt vervuld door een medewerker uit het atelier. De contactpersoon is het verlengstuk van de Privacy Officer naar de medewerkers en treedt op als 1e contactpunt bij privacy vraagstukken. Afhankelijk van grootte van het atelier of complexiteit van de processen kan de contactpersoon nog worden ondersteund door meer ervaren medewerkers binnen het atelier. De belangrijkste taken zijn:

- Het beoordelen van de verwerking(en) van persoonsgegevens tegen de achtergrond van de kaders van de AVG en de sectorale wetgeving;
- Het adviseren van medewerkers over de toepassing van de AVG en beantwoorden van eenvoudige privacyvraagstukken, het bijdragen aan het privacy bewustzijn;
- Adviseren en ondersteunen bij het definiëren van verwerkersovereenkomsten en het onderhouden van het verwerkingsregister.