Uitvoeringsbeleid Gegevensbescherming

Gemeente Maastricht

Inleiding

De gemeente Maastricht verwerkt bij het uitvoeren van haar taken veel persoonsgegevens. Wij vinden het belangrijk dat betrokkenen erop kunnen vertrouwen dat hun persoonsgegevens bij onze organisatie in goede handen zijn. Als gemeente hechten wij veel waarde aan integriteit en het zorgvuldig omgaan met persoonsgegevens maakt dan ook deel uit van ons het integriteitsbeleid en de bijhorende gedragscode.

Aanleiding

De inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) is de belangrijkste reden voor het opstellen van dit Uitvoeringsbeleid Gegevensbescherming. In deze nieuwe Europese privacywet worden de regels voor de bescherming van persoonsgegevens aangescherpt en uitgebreid zodat deze beter aansluiten op de toegenomen digitalisering van onze samenleving.

Deze verordening maakt ons (nog) bewuster van het belang van privacybescherming en de risico's van het verwerken van persoonsgegevens. Deze wet dwingt ons om bij nieuwe ontwikkelingen de gevolgen voor de privacy van betrokkenen mee te nemen in de besluitvorming en om vanaf het begin na te denken over privacybeschermende en verhogende maatregelen.

De AVG zorgt voor een verstrekking van de privacyrechten aan betrokkenen. Zij dienen meer controle te krijgen over hun persoonsgegevens. Bovendien krijgen organisaties die persoonsgegevens verwerken (verwerkingsverantwoordelijke) onder de AVG een verantwoordingsplicht. Zij dienen op basis van documenten te kunnen aantonen dat zij voldoen aan de wettelijke verplichtingen (accountability).

Met dit uitvoeringsbeleid willen wij aangeven hoe wij als gemeentelijke organisatie omgaan met persoonsgegevens en de privacy van betrokkenen waarborgen. Het beleid is van toepassing op de hele organisatie.

Naast dit gemeentebrede kapstokbeleid zal er, samen met de betreffende organisatieonderdelen, themabeleid worden ontwikkeld voor die plekken binnen de organisatie waar veel en/of gevoelige persoonsgegevens worden verwerkt.

1. Uitgangspunten voor het verwerken van persoonsgegevens

De AVG bevat een aantal duidelijke en goede uitgangspunten voor het verwerken van persoonsgegevens. Logischerwijs vormen deze punten ook de basis voor dit Uitvoeringsbeleid Gegevensbescherming.

1.1. Rechtmatigheid

Persoonsgegevens mogen alleen worden verwerkt als hiervoor een rechtmatige grondslag in de AVG is opgenomen. De belangrijkste grondslagen voor het verwerken van persoonsgegevens door onze gemeente zijn het uitvoeren van een wettelijke verplichting of van een bij wet geregelde taak van algemeen belang.
Voorbeelden van gegevensverwerkingen op basis van een wettelijke verplichting zijn het verstrekken van een omgevingsvergunning of een uitkering op grond van de Participatiewet. Een voorbeeld van een bij wet vastgelegde taak van algemeen belang waarvoor persoonsgegevens worden verwerkt, is de behandeling van klachten. Voor het verwerken van persoonsgegevens in het kader van onze privaatrechtelijke taken of door de culturele instellingen en Maastricht Sport, kan gebruik worden gemaakt van de grondslag 'het uitvoeren van een overeenkomst'.
Verder dient de verwerking van persoonsgegevens te voldoen aan de beginselen van proportionaliteit en subsidiariteit.

Wat betekent dit in de praktijk?

- Onze organisatie verwerkt alleen de persoonsgegevens die noodzakelijk zijn voor het te bereiken doel (proportionaliteit);
- Het verwerken van persoonsgegevens gebeurt op een dusdanige wijze dat de gevolgen voor de privacy van betrokkene zo beperkt mogelijk blijven (subsidiariteit);
- De in de AVG opgenomen verwerkingsgrondslag 'toestemming van betrokkene' wordt zeer beperkt toegepast en niet gehanteerd bij de uitvoering van wettelijke taken. De AVG bepaalt namelijk dat er bij toestemming sprake dient te zijn van een gelijkwaardige relatie tussen betrokkene en de organisatie waaraan de toestemming wordt gegeven. Wij zijn ons ervan bewust dat deze gelijkwaardige relatie tussen betrokkene en de gemeente zelden aanwezig is. De belangrijkste uitzondering op deze regels is het verwerken van persoonsgegevens bij aanmeldingen voor nieuwsbrieven. In dat geval zal altijd expliciet toestemming aan betrokkene worden gevraagd.

1.2. Behoorlijkheid

De gemeente verwerkt alleen persoonsgegevens die noodzakelijk zijn voor het doel van de verwerking (minimale gegevensverwerking). Hierbij geldt als uitgangspunt dat de hulpvraag van betrokkene leidend is bij het verzamelen en verder verwerken van persoonsgegevens. De gegevens worden niet langer bewaard dan noodzakelijk is. Het doel van de verwerking en/of de van toepassing zijnde wet bepalen de noodzakelijke bewaartermijn.

Wat betekent dit in de praktijk?

- Het beginsel ‘eenmalige vastlegging en meervoudig gebruik’ van persoonsgegevens wordt gehanteerd voor de gegevens die zijn opgenomen in basisregistraties;
- Persoonsgegevens zullen nooit worden gebruikt voor commerciële doeleinden.
- Medewerkers hebben alleen toegang tot persoonsgegevens die noodzakelijk zijn voor de uitoefening van hun werkzaamheden. De in-, door- en uitstroomprocedures waarborgen dat de verstrekte autorisaties actueel zijn. Er zal periodiek een audit worden gehouden waarin de werking van deze procedures worden getoetst
- Wanneer dit noodzakelijk is, zal er een Gegevensbeschermingseffectbeoordeling (DPIA)[1] worden uitgevoerd voordat er met een verwerking wordt gestart;
- In de samenwerkingsverbanden waaraan onze organisatie deelneemt, zullen afspraken worden gemaakt over de verwerking van persoonsgegevens;
- Er wordt gewerkt volgens het verplichte AVG-principe van *privacy by design* (zie paragraaf 3) en de landelijke afspraken voor informatiebeveiliging voor gemeenten[2];
- Waar mogelijk worden (nieuwe) systemen dusdanig ingericht dat bewaartermijnen hierin zijn opgenomen (harde wettelijke termijnen) en er een signaal wordt afgegeven wanneer stukken dienen te worden gearchiveerd of vernietigd.

1.3. Transparantie

De gemeente is transparant richting betrokkenen en informeert hen in begrijpelijke taal over de wijze waarop met persoonsgegevens wordt omgegaan. De gemeente zorgt er daarnaast voor dat burgers optimaal worden gefaciliteerd als zij gebruik willen maken van de rechten die de AVG hun geeft.

Wat betekent dit in de praktijk?

- De gemeentelijke website bevat een pagina ‘privacy’ met informatie voor betrokkenen over de bescherming van persoonsgegevens, hun rechten en formulieren om van deze rechten gebruik te maken;
- Een samenvatting van het gemeentelijk verwerkingsregister is gepubliceerd op de gemeentelijke website.
- Medewerkers zullen door middel van bewustwordingscampagnes en trainingen zoals e-learningmodules, voortdurend worden geïnformeerd over het zorgvuldig verwerken van persoonsgegevens. Ook zullen zij een bij hun werkzaamheden passende voorlichting krijgen over het omgaan met persoonsgegevens. Het intranet heeft een pagina ”privacybescherming” met informatie over de AVG en te gebruiken formats.
- In de jaarrekening zal worden gerapporteerd over de stand van zaken betreffende de bescherming van persoonsgegevens.

[1] Zie bijlage 2 voor een toelichting over de DPIA (afkorting is afgeleid van de Engelse term Data Protection Impact Assessment).
[2] Deze afspraken zijn opgenomen in de Baseline Informatiebeveiliging voor de Overheid (BIO).

2. Borging van verantwoordelijkheden en taken in de organisatie

2.1. Verantwoordelijkheden

Binnen de gemeente Maastricht is de (informele) verwerkingsverantwoordelijkheid op verschillende plekken in de organisatie belegd. Met dit uitvoeringsbeleid wordt expliciet vastgelegd hoe de AVG-taken en verantwoordelijkheden binnen onze organisatie zijn verdeeld.

2.1.1. Verwerkingsverantwoordelijke

De meeste verwerkingen van persoonsgegevens in onze organisatie vinden plaats onder de verwerkersverantwoordelijkheid van het college van B&W.
In deze hoedanigheid is het college er voor verantwoordelijk dat iedere verwerking van persoonsgegevens rechtmatig is en voldoet aan het proportionaliteits- en subsidiariteitsbeginsel. Bovendien dient de verwerkingsverantwoordelijke ervoor te zorgen dat er passende maatregelen worden getroffen om de gegevens te beschermen.
De andere verwerkingsverantwoordelijke organen binnen de gemeentelijke organisatie zijn de burgemeester en de gemeenteraad.

2.1.2. Verantwoordelijkheid op directieniveau

De gemeentesecretaris is als algemeen directeur van de ambtelijke organisatie eindverantwoordelijk voor de bedrijfsvoering, waaronder het verwerken van persoonsgegevens. De gemeente Maastricht heeft een directieteam en binnen dit team ligt de bovengenoemde verantwoordelijkheid bij de directeur bedrijfsvoering en dienstverlening. Deze directeur is tevens verantwoordelijk voor het melden van datalekken.

2.1.3. Verantwoordelijkheid op managementniveau

De managers (bedrijfsvoering) zijn binnen het organisatieonderdeel verantwoordelijk voor de naleving van de AVG en dit uitvoeringsbeleid. Zij zorgen ervoor dat:

- De teams de AVG naleven en inbedden in de werkprocessen van hun team;
- Er binnen hun organisatieonderdeel voldoende deskundigheid is over de bescherming van persoonsgegevens (zie ook paragraaf 2.1.5.);
- De *quick scan privacy* wordt doorlopen, onder andere bij beleidsontwikkelingen en aanschaf van nieuwe systemen, waarbij sprake is van verwerking van persoonsgegevens
- Het verwerkingsregister actueel wordt gehouden voor de werkprocessen van het organisatieonderdeel;
- Indien noodzakelijk, voorafgaande aan de verwerking, een Gegevensbeschermingseffect-beoordeling (DPIA), wordt uitgevoerd;
- Passende organisatorische- en technische maatregelen worden genomen om de persoonsgegevens te beveiligen;
- De verzoeken van betrokkenen conform de wettelijke eisen worden afgehandeld;
- Betrokkenen in duidelijke en eenvoudige taal worden geïnformeerd, onder meer op de website, over de persoonsgegevens die door het organisatiedeel worden verwerkt;
- Bij (mogelijke) datalekken conform de vastgestelde procedure ‘meldplicht datalekken’ wordt gehandeld;

- De in-, door- en uitstroomprocedures worden nageleefd, en de medewerkers bij uitstroom de verstrekte gegevensdragers inleveren en hun persoonlijke schijf en mailbox hebben opgeschoond.

In de reguliere verantwoordingscyclus voor het management wordt ook de verantwoording over het gebruik van persoonsgegevens opgenomen.

2.1.4. Functionaris Gegevensbescherming (FG)

Deze functionaris dient er binnen een organisatie op toe te zien dat wordt voldaan aan de wettelijke verplichtingen uit de AVG. Als verplichte interne toezichthouder voor de gegevensbescherming rapporteert deze medewerker aan het college van B en W. Conform de AVG zal de FG tijdig worden betrokken bij ontwikkelingen en vraagstukken die raakvlakken hebben met de bescherming van persoonsgegevens. Verder houdt de functionaris gegevensbescherming onder meer het 'datalek register' bij en is hij verantwoordelijk voor de afhandeling van ingediende klachten betreffende de privacybescherming.

De functionaris gegevensbescherming zal vooral blijven fungeren als adviseur en sparringpartner voor de organisatie bij het naleven van de privacywetgeving. Daarnaast zorgt de FG ervoor dat de privacybescherming en de AVG bij de medewerkers onder de aandacht blijft. Voor de informatiebeveiliging rond persoonsgegevens laat deze functionaris zich adviseren door de *Chief Information Security Officer* (CISO).

2.1.5. AVG-contactpersoon

Ieder organisatieonderdeel zal één of meer AVG-contactpersonen aanwijzen. Deze medewerker is binnen het organisatieonderdeel het eerste aanspreekpunt voor vragen van medewerkers en management over de AVG en het verwerken van persoonsgegevens.
De contactpersoon adviseert de teammanagers over de toepassing van de AVG bij de uitvoering van de reguliere werkzaamheden en draagt zorg voor de operationele AVG werkzaamheden in zijn organisatieonderdeel, zoals het bijhouden van het verwerkingsregister.

De FG vervult een coördinerende rol. Hij zal op reguliere basis overleg voeren met iedere AVG-contactpersoon. Daarnaast komen deze contactpersonen onder leiding van de functionaris gegevensbescherming regelmatig bij elkaar om kennis te delen en ervoor te zorgen dat gemeente-breed op uniforme wijze wordt omgegaan met persoonsgegevens.

Deze werkwijze sluit grotendeels aan bij de door de VNG voorgestelde organisatorische inbedding van de AVG binnen gemeenten. De VNG adviseert om naast de verplichte functie van FG een gemeentebrede privacy adviseur te benoemen en voor ieder onderdeel een privacy ambassadeur aan te wijzen (AVG-contactpersonen). Vooralsnog heeft onze organisatie geen privacyadviseur benoemd. Deze taken zullen derhalve worden uitgevoerd door de AVG-contactpersonen en de functionaris gegevensbescherming.
In overleg met het managementteam van ieder organisatieonderdeel wordt de formatieomvang voor de AVG-contactpersonen bepaald. Na een jaar zal dit worden geëvalueerd.

2.1.6. Medewerkers

Iedere medewerker dient bij het uitvoeren van zijn functie zorgvuldig om te gaan met persoonsgegevens en is verplicht alle zaken waarvan hij weet of vermoedt dat ze een vertrouwelijk karakter hebben, geheim te houden. Met het afleggen van de ambtseed verklaren de medewerkers verklaren dat zij zich aan deze verplichting zullen houden.
Medewerkers die geen ambtelijke aanstelling hebben, zullen een integriteitsverklaring en geheimhoudingsverklaring ondertekenen.

3. De quick scan privacy

De in te voeren quick scan privacy[3] helpt de organisatie bij het naleven van een tweetal nieuwe wettelijke verplichtingen: privacy by design en de gegevensbeschermingseffectbeoordeling (DPIA).

Werken volgens het principe van *privacy by design* houdt in dat er vanaf de ontwikkelfase van beleid, producten en/of systemen voortdurend proactief maatregelen worden genomen om de privacy van de betrokkenen te waarborgen en niet meer gegevens te verwerken dan noodzakelijk is.

De *quick scan* privacy is een hulpmiddel om aan deze wettelijke eis te voldoen. Door het uitvoeren van deze scan wordt duidelijk of een verwerking is toegestaan, welke de eventuele risico's zijn en welk pakket van maatregelen daarbij past om te voldoen aan het vereiste beschermingsniveau.

Tevens kan *quick scan* worden beschouwd als een verkorte DPIA. Door het invullen van de quick scan privacy wordt duidelijk of een (volledige) DPIA noodzakelijk is. De betrokken manager en de functionaris gegevensbescherming kunnen namelijk op basis van de resultaten uit de *quick scan bepalen* of een verplichte DPIA dient te worden uitgevoerd.
De quick scan wordt bewaard bij de FG zodat deze kan aantonen hoe onze organisatie de rechtmatigheid en risico's van nieuwe en aangepaste verwerkingen toetst.

4. Beveiliging

4.1. Beveiligingsmaatregelen

Bij het verwerken van persoonsgegevens door of namens de gemeente dragen wij zorg voor passende beveiligingsmaatregelen die gelet op aard van de verwerking/gevoeligheid van de gegevens een op het risico afgestemd beveiligingsniveau bevatten.

4.2. Meldplicht datalekken

Een datalek is een beveiligingsprobleem dat ontstaat door een inbreuk op de beveiligingsmaatregelen waarbij, per ongeluk of met opzet, persoonsgegevens in verkeerde handen terecht komen of verloren gaan.

[3] Zie bijlage 2

De AVG verplicht ons om datalekken die een risico vormen voor de privacybescherming van betrokkenen[4] binnen 72 uur na ontdekking van het lek, te melden bij de Autoriteit Persoonsgegevens (AP). Als dit risico heel erg hoog is, dienen ook de betrokkenen waarvan de persoonsgegevens zijn gelekt, te worden geïnformeerd. Een voorbeeld van een hoog risico is het lekken van gegevens die kunnen worden gebruikt voor identiteitsfraude of uitsluiting van bepaalde groepen.

De gemeente Maastricht heeft voor het tijdig en adequaat reageren op een datalek de procedure 'Meldplicht datalekken' opgesteld. Deze procedure is gepubliceerd op intranet en zal herhaaldelijk bij de medewerkers onder de aandacht worden gebracht. Iedereen die denkt een datalek te hebben ontdekt, dient dit onmiddellijk te melden bij de Servicedesk.

Conform de AVG wordt ieder jaar een register bijgehouden van alle datalekken die gedurende dat jaar hebben plaatsgevonden, ongeacht of deze zijn gemeld bij de Autoriteit Persoonsgegevens.

5. Verwerkingsregister

De FG beheert namens de verwerkingsverantwoordelijke het wettelijk verplichte verwerkingsregister dat een actueel overzicht bevat van de door onze organisatie uitgevoerde verwerkingen van persoonsgegevens. Ieder organisatieonderdeel is verantwoordelijk voor de juistheid en het actueel houden van zijn eigen onderdeel in dit register. De FG houdt toezicht op de rechtmatigheid van de in het register opgenomen verwerkingen van persoonsgegevens.

6. Verwerkersovereenkomst

Indien de organisatie voor het uitvoeren van gemeentelijke taken waarbij persoonsgegevens worden verwerkt een verwerker inschakelt, wordt met deze partij een verwerkersovereenkomst afgesloten. Hiervoor wordt gebruik gemaakt van de door onze organisatie opgestelde standaardovereenkomst of, indien van toepassing, de verwerkersovereenkomst van de VNG.
Conform het informatiebeveiligingsbeleid worden er alleen opdrachten gegeven aan verwerkers die aantoonbaar (certificering, TPM-verklaring) voldoende garanties kunnen bieden voor de beveiliging van onze persoonsgegevens.

Indien de gemeente persoonsgegevens uitwisselt met een externe partij die geen verwerker is, worden passende afspraken vastgelegd om te waarborgen dat er zorgvuldig met deze gegevens wordt omgegaan. Bijvoorbeeld over het versleuteld verzenden van e-mailberichten met persoonsgegevens.

7. Ter afsluiting

Dit uitvoeringsbeleid wordt gepubliceerd op het gemeentelijke intranet. Verder zullen de inhoud en naleving van dit beleid op reguliere basis aan bod komen in de managementteam overleggen van de

[4] In de richtlijnen meldplicht datalekken van de Autoriteit Persoonsgegevens wordt aangegeven wanneer sprake is van een dergelijk risico.

organisatieonderdelen. De organisatieonderdelen zullen deze gemeentebrede beleidskaders in samenwerking met de FG, waar nodig, doorvertalen naar organisatieonderdeel specifiek beleid en/of werkinstructies.

Bijlage 1. Quick scan privacy

- Naam van de voorgenomen verwerking van persoonsgegevens:

- Voor welk doel worden de persoonsgegevens verwerkt?

- Is dit een wettelijke verplichting? Zo ja, welke verplichting?

- Is dit een publiekrechtelijke taak? Uit welk wet (ten) volgt deze taak?

- Wordt er gebruikgemaakt van een bestaande verzameling van persoonsgegevens?
  Zo ja, welke verzameling?

- Hoelang worden de gegevens bewaard? Is er een wettelijke bewaartermijn?

- Worden de gegevens gedeeld met andere instanties of binnen een samenwerkingsverband?

- Wordt er gebruik gemaakt van een Verwerker (taak uitbesteed aan een externe organisatie/ persoonsgegevens opgeslagen in de Cloud/SaaSoplossing?

	Overige Vragen	Ja (*toelichten)*	Nee	Onbekend
1	Zullen er bijzondere persoonsgegevens verwerkt worden? (Medische gegevens, justitiële gegevens, ras, levensovertuiging, seksuele voorkeur, lidmaatschap vakbond			
2	Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?			
3	Zal het BSN-nummer of een ander persoonsgebonden nummer verwerkt worden?			
4	Zullen gegevens uitgewisseld worden met andere gekoppelde informatiesystemen?			

Een Gegevensbeschermings effect beoordeling (DPIA) is in elk geval nodig als bij vraag 1 +2 Ja of Onbekend is ingevuld

Manager (bedrijfsvoering):

Ingevuld door/functie:

Bijlage `2. Gegevensbeschermingseffectbeoordeling (DPIA)

Onder de Algemene Verordening Gegevensbescherming (AVG) kunnen organisaties verplicht zijn een gegevensbeschermingseffectbeoordeling uit te voeren. Veelal wordt dit aangeduid met de Engelstalige afkorting DPIA (*Data Protection Impact Assessment*). Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. Aan de hand van de resultaten zal worden bepaald of de gegevensverwerking rechtmatig is en of er aanvullende beveiligingsmaatregelen dienen te worden genomen.

De AVG geeft aan dat een DPIA verplicht is, als een nieuwe of gewijzigde gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de persoonsgegevens verwerkt gaan worden. Of van een hoog privacyrisico sprake is, dient de verwerkingsverantwoordelijke zelf te bepalen.

In de AVG is vastgelegd dat er in ieder geval een DPIA moet worden uitgevoerd als een organisatie:

- besluiten over betrokkenen neemt zonder menselijke tussenkomst, maar deze baseert op geautomatiseerde verwerkingen van persoonsgegevens, eventueel met behulp van standaardprofielen (bijvoorbeeld een algoritme dat bepaalt of de lening kan worden verstrekt);
- op grote schaal bijzondere persoonsgegevens verwerkt of strafrechtelijke gegevens verwerkt;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld door middel van cameratoezicht).

De Autoriteit Persoonsgegevens heeft daarnaast met de andere Europese toezichthouders een lijst[5] van soorten verwerkingen opgesteld waarvoor het uitvoeren van een DPIA, voorafgaande aan de verwerking ook verplicht is. Dit betreft ondermeer:

1. Heimelijk onderzoek
2. Gezondheidsgegevens
3. Fraudebestrijding
4. Cameratoezicht/ flexibel cameratoezicht
5. Financiële situatie
6. Genetische persoonsgegevens en/of biometrische gegevens
7. Samenwerkingsverbanden
8. Controle werknemer
9. Prrofiling
10. Monitoring en beïnvloeding van gedrag

De lijst is niet uitputtend. Als de gemeente een verwerking wenst uit te voeren die niet op deze lijst staat of expliciet is opgenomen in de wet, dient zijzelf te beoordelen of de verwerking een hoog privacyrisico oplevert. Voor deze beoordeling kan gebruik worden gemaakt van de 9 criteria[6] die

[5] De lijst inclusief toelichting is te vinden op: https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667

[6] https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-europese-privacytoezichthouders-6668.

eveneens door de Europese privacy toezichthouders zijn opgesteld. Als uitgangspunt geldt dat wanneer aan tenminste 2 criteria wordt voldaan, een DPIA moet worden uitgevoerd.

Indien een DPIA noodzakelijk is, mag er niet worden begonnen met de gegevensverwerking voordat deze is uitgevoerd en de eventueel vereiste maatregelen zijn getroffen.

Voor het uitvoeren van een DPIA zijn geen strikte voorschriften in de regelgeving opgenomen. De verantwoordelijke voor de gegevensverwerking moet natuurlijk zorgen voor een gedegen aanpak. De AVG schrijft voor dat de Functionaris Gegevensbescherming (FG) bij iedere DPIA om advies dient te worden gevraagd.