Gemeente Maastricht

> RETOURADRES POSTBUS 1992, 6201 BZ MAASTRICHT

Aan de raadsfractie CDA
Mevr. V. Heijnen

BEZOEKADRES
Mosae Forum 10
6211 DW Maastricht

POSTADRES
Postbus 1992
6201 BZ Maastricht

WWW.GEMEENTEMAASTRICHT.NL

ONDERWERP
Vragen art. 48 RvO privacy CDA

DATUM
10 februari 2015

VERZONDEN 12 FEB. 2015

BIJLAGEN
1

BEHANDELD DOOR
R.Dirx

DOORKIESNUMMER
043 350 4227

ONZE REFERENTIE
2015-03900

E-MAILADRES
raymond.dirx@maastricht.nl

FAXNUMMER
043 350 42 30

UW REFERENTIE

Geachte meneer/mevrouw,

Onderstaand treft u de beantwoording aan van de vragen die uw fractie gesteld heeft in het kader van art. 48 van het Reglement van Orde.

Vraag 1: Kunt u ons duidelijk maken hoe u de privacy van onze burgers heeft geborgd in uw beleid? Graag ontvangen wij van u alle beleidsstukken die daar betrekking op hebben.

Antwoord 1:
Het college heeft privacy van de burgers geborgd door toepassing van de Wet Bescherming Persoonsgegevens (Wbp) en daarvan afgeleid de door de raad vastgestelde privacyverordening.

Tevens is een functionaris gegevensbescherming (FG) benoemd door het college. Deze FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Wbp. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie binnen de organisatie. Hiermee voldoet de gemeente aan de eisen en is zelfregulerend. College Bescherming Persoonsgevens (CBP) heeft een toezichthoudende rol op de uitvoering van de Wbp.

De FG adviseert gevraagd en ongevraagd over de toepassing van de Wbp binnen de organisatie en houdt een openbaar register bij van alle verwerkingen van persoonsgegevens binnen de gemeente Maastricht. De FG is het aanspreekpunt voor alle zaken die de bescherming van de persoonlijke levenssfeer aangaan. Inwoners, klanten, personeelsleden, kortom alle betrokkenen van wie persoonsgegevens worden verwerkt, kunnen bij de FG terecht voor informatie over en inzage in de van hem of haar verwerkte gegevens. Ook is de FG het aanspreekpunt voor vragen en opmerkingen over de eigen verwerkte gegevens.

De FG adviseert ook over de informatiebeveiliging in de gemeentelijke organisatie. De FG sluit derhalve ook regelmatig aan bij het interne informatiebeveiligingsoverleg van onze organisatie. De afgelopen jaren heeft er een verdere professionalisering van de FG functie plaatsgevonden. (Doel, taken en verantwoordelijkheden en activiteiten van de functie zijn

duidelijker gemaakt. Zo is er inmiddels een eigen intranetsite met daarop uitleg, richtlijnen en hulpmiddelen, etc. om een juiste toepassing van de Wbp te faciliteren. Aanvullend is een uitgangspunt van informatiebeveiliging, daar waar nodig, de waarborging van beschikbaarheid, integriteit en vertrouwelijkheid van gegevens).
In bijlage treft u aan de privacyverordening gemeente Maastricht.

Vraag 2: In hoeverre hebt u de landelijke richtlijnen van de VNG opgevolgd?

Antwoord 2:
Ons college volgt de richtlijnen van de VNG. Een van de voorbeelden, waarbij de richtlijnen van de VNG aantoonbaar zijn gevolgd, is de Diginotar. Toendertijd zijn de communicatie, richtlijnen en adviezen vanuit de VNG voor wat betreft het wel of niet afsluiten van bepaalde diensten van ons digitale loket door de mogelijke onveiligheid van DigiD geheel door ons gevolgd.
Verder participeert de gemeente Maastricht sinds het begin in een intergemeentelijke expertise groep die mede aan de basis heeft gestaan van de oprichting van de Informatiebeveiligingsdienst (IBD). Vanuit de IBD vindt continuering van deze expertise groep plaats. De gemeente Maastricht is hierbij nog steeds één van de deelnemers. Hier zijn we niet "slechts" volgend. Onze medewerkers participeren in landelijk overleg en denken mee bij het ontwerpen van dergelijke richtlijnen. Een voorbeeld hiervan is de strategische en tactische Baseline Informatiebeveiliging Nederlands Gemeenten (BIG) en de hieronder liggende operationele producten.

Vraag 3: Is uw organisatie voorbereid op het volledige aanbod van en werkt zij samen met de informatiebeveiligingsdienst (IBD)?

Antwoord 3:
Ja. Maastricht heeft als één van de eerste gemeenten aansluiting gezocht bij de IBD. Alle stappen van het aansluitproces, zoals benoemd in onderstaande tabel, bij de IBD zijn snel en adequaat doorlopen.

Nr	*Stap*	*Resultaat*
1	Aanstellen ACIB (aanstellen van een Algemene Contactpersoon Informatiebeveiliging (ACIB))	• Waarschuwingen en informatie met een niet vertrouwelijk karakter over algemene bedreigingen en incidenten. • Mogelijkheid om incidenten te melden bij de IBD.
2	Aanstellen VCIB (aanstellen van een Vertrouwde Contactpersoon Informatiebeveiliging (VCIB))	• Waarschuwingen en informatie met een vertrouwelijk karakter over mogelijke bedreigingen en incidenten. • Mogelijkheid om incidenten waarbij ook vertrouwelijke gegevens worden uitgewisseld, te melden bij de IBD.
3	Doorgeven IP-adressen en URL's	• Waarschuwingen over mogelijk geïnfecteerde systemen.
4	Aanleveren gemeentelijke ICT-foto	• IBD kwetsbaarheidswaarschuwingen op maat over mogelijke kwetsbaarheden in hard en software.

De gemeente Maastricht is dus volledig aangesloten en kan hierdoor gebruik maken van het volledige dienstenaanbod van de IBD. We maken ook feitelijk regelmatig gebruik van hun diensten en werken nauw met de IBD samen.

Vraag 4: Hebt u aan de hand van Baseline (gemeenschappelijk normenkader) de informatie-beveiliging binnen de organisatie op orde en waaruit blijkt dat?

Antwoord 4:
Het college heeft in 2009 het informatiebeveiligingsbeleid, gebaseerd op de Code voor Informatiebeveiliging vastgesteld. Informatiebeveiliging is inmiddels structureel verankerd binnen de organisatie.Verantwoordelijkheden zijn daarbij op alle lagen belegd. Dit is vastgelegd in een informatiebeveiligingsplan en informatiebeveiligingsorganisatie document. Onderdeel hiervan is ook een structureel informatiebeveiligingsoverleg. Hierin nemen van belang zijnde functionarissen plaats en daar waar nodig zullen voor bepaalde casussen specifieke expertises en/of leidinggevenden aanhaken. Binnen dit overleg worden alle lopende en nieuwe zaken aangaande informatiebeveiliging besproken. Dit kan variëren van incidenten/problemen, projecten/aanbestedingen tot de implementatie van

beveiligingsmaatregelen, etc.. Daarnaast wordt deze bijeenkomst ook gebruikt als themabijeenkomst om een specifiek thema of een actualiteit samen met een specifieke doelgroep te bespreken.
De gemeentelijke organisatie gebruikt periodiek een aantal toetsingen/beoordelingen ten aanzien van informatiebeveiliging zoals, interne/externe securtiytesten jaarlijks ICT beveiligingsassement DigiD, Automatisering/informatiebeveiliging in het kader van de P&C cyclus/jaarrekeningcontrole.
Zoals gezegd is de aansluiting bij de IBD op orde waardoor wij volledig en actief gebruik maken van hun producten zoals incidentpreventie, incidentdetectie en incidentcoördinatie.
Door het definitief vorm krijgen van de landelijke strategische en tactische Baseline Informatiebeveiliging Nederlands Gemeenten (BIG) zal de gemeente Maastricht in 2015 toewerken naar de vaststelling van een nieuw informatiebeveiligingsbeleid dat als basis deze baselines heeft. Dat is vooral een formele aanpassing van het beleid om daarbij aan te sluiten bij nieuwe definities en terminolgie uit de BIG . Naar verwachting zal dit nieuwe beleid er niet toe leiden dat de bestaande uitvoeringspraktijk substantieel wijzigt.

Vraag 5 .Welke afweging en prioritering heeft u van dit normenkader onderbouwd?

Antwoord 5:
Zoals benoemd is vanuit het vastgestelde informatiebeveiligingsbeleid verdere invulling gegeven aan informatiebeveiliging in ondermeer een informatiebeveiligingsplan. Dit informatiebeveiligingsplan geeft aan hoe de focus en aanpak voor de gemeente Maastricht eruit ziet. Hierbij zijn ook de aspecten doelmatigheid en doeltreffendheid van belang geweest.
Door het definitief worden van de BIG en de totstandkoming van de VNG resolutie wordt nieuw beleid opgesteld in lijn met de BIG en resolutie. Van hieruit wordt vervolgens een nieuwe prioriteitstelling opgesteld door het formuleren van een nieuw (uitvoerings)plan.

Vraag 6: Welke borging heeft u doen plaatsvinden om zelfregulering vorm te geven?

Antwoord 6:
Aan het proces om te komen tot een hoge mate van zelfregulering wordt momenteel door de IBD en Taskforce Bestuur en Informatieveiligheid Dienstverlening (taskforce BID) in samenwerking met gemeenten steeds verder invulling gegeven. Uitgangspunten voor de uitwerking zijn:

1. Een gemeenschappelijk normenkader moet als basis dienen. Bepaald moet worden of de BIG dit gemeenschappelijke normenkader kan worden.

De gemeente Maastricht is actief betrokken geweest bij de opstelling van de baselines als gemeenschappelijk normenkader en onderstreept het belang hiervan.

2. Lokaal moet informatiebeveiligingsbeleid worden vastgesteld. Met gebruik van het gemeenschappelijke normenkader maakt de gemeente een afweging en prioritering,onderbouwd vanuit een eigen nul-meting.

De gemeente Maastricht heeft al beleid, een plan en een organisatie voor informatiebeveiliging. De gemeente Maastricht zal in 2015 toewerken naar de vaststelling van een nieuw informatiebeveiligingsbeleid dat als basis deze baselines heeft. Naar verwachting zal dit nieuwe beleid er niet toe leiden dat de bestaande uitvoeringspraktijk

substantieel wijzigtBorging moet plaats vinden door zelfregulering vorm te geven middels een interne cyclus, door transparantie, collegiale toetsing en een vorm van extern toezicht.
Zie antwoord vraag 7 hieronder

Vraag 7: Kunt u aangeven of deze vorm heeft gekregen middels een interne cyclus, door transparantie, collegiale toetsing en of een vorm van extern toezicht en/of de verplichte audit? Wij zien de audit gaarne tegemoet.

Antwoord 7:
De gemeente heeft een organisatie ingericht met structureel informatiebeveiligingsoverleg. Verder vinden er zowel intern als extern (verplichte) toetsingen plaats. Voorbeelden hiervan zijn ICT beveiligingsassement DigiD, penetratietesten en vulnerabilityscans (scans op zwakheden in onze IT-infrastructuur). Ook zijn binnen de organisatie hier medewerkers voor opgeleid, zoals Certified Ethical Hacker (CEH), EC-Council Certified Security Analyst (ECSA), Licensed Penetration Tester (LPT), Certified Information Systems Security Professional (CISSP). Hierbij is deze deskundigheid niet alleen van belang voor toetsing(achteraf) maar ook aan de voorkant bij de inrichting van onze ICT-infrastuctuur. Naast organisatorische en technische maatregelen is een andere zeer belangrijk aspect de medewerkers zelf. Awareness creëren bij en communicatie richting de medewerkers aangaande informatiebeveiliging en bijvoorbeeld incidenten hieromtrent zijn dan ook van belang en gebeurt ook. In 2014 is een aanbestedingstraject gestart voor het uitvoeren van een nieuwe, gemeentebrede, awarenesscampagne om het bewustzijn (en zelfregulering) bij medewerkers te verhogen. Indien gewenst is, (wegens vertrouwelijkheid) inzage mogelijk voor de raadsleden in de rapportage van het verplichte jaarlijkse ICT beveiligingsassessment DigiD. Dit is de rapportagevorm zoals deze ook verstrekt wordt aan het Logius (ministerie BZK).

Vraag 8: Kunt u ons laten zien hoe u het verplichte ICT-Beveiligingsassessment DigiD toepast?

Antwoord 8:
Het afgelopen jaar heeft de gemeente Maastricht het ICT-Beveiligingsassessment DigiD, een jaarlijks terugkerend beveiligingsonderzoek, opgelegd door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, succesvol afgerond en tijdig gerapporteerd richting Logius (ministerie BZK).

Indien gewenst is, wegens vertrouwelijkheid, voor de raadsleden inzage mogelijk in het plan aanpak van hoe deze toetsing binnen de gemeente is uitgevoerd.

Vraag 9: Bent u het met ons eens dat onze gemeente en samenwerkende gemeenten (gezien de grote concentratie van informatie in dergelijke samenwerkingsverbanden) scherp moeten zijn op de potentiële risico's die zij lopen en welke preventieve maatregelen u heeft genomen om deze uit te bannen?

Antwoord 9:
Ja, dat zijn wij met u eens. Wij zijn ons te allen tijde bewust van de risico's die het beheer en uitwisseling van informatie met zich meebrengt. Het eigenaarschap van bepaalde informatie

is niet enkel beperkt tot de aanwezigheid van deze informatie binnen de eigen organisatie. Ook in het geval van overdragen van en/of delen van informatie dienen de kwaliteitsaspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid voorop te staan. Daar, waar in het kader van privacy noodzakelijk, worden bijvoorbeeld via een verhoogd beveiligingsniveau (encryptie etc.) gegevens uitgewisseld.

Vraag 10: Kunt u ons verzekeren dat collegebesluiten nooit geantedateerd zijn?

Antwoord 10:
Ja.

We gaan ervan uit we met bovenstaande antwoorden de bij u gerezen twijfels over de kwaliteit van onze gemeentelijke informatiebeveiliging hebben kunnen wegnemen.

Met vriendelijke groet,
Namens het college van burgemeester en wethouders van Maastricht,

John Aarts,
Wethouder Economie, Mobiliteit en Financiën.

Raadsvergadering: 17-02-2009
Agendapunt: 5.2
Beslissing: Conform.
Toezegging: -

VOLGNUMMER	DATUM	DOMEIN
11-2009	27 januari 2009	PID
CORRESPONDENTIENUMMER	BIJLAGEN	RAADSCOMMISSIE
2009.01343	1	Algemene Zaken, Openbare Orde en Veiligheid
ONDERWERP RAADSNOTA		STELLER
Privacyverordening		Graven/350 5855 charlotte.graven@maastricht.nl

AAN DE GEMEENTERAAD

1. Doel van het raadsvoorstel, samenvatting en besluiten

Ter naleving van de Wet bescherming persoonsgegevens de Privacyverordening Gemeente Maastricht vast te stellen.

2. Situatie / aanleiding / probleem

De wijze waarop de implementatie van de Wet bescherming persoonsgegevens wordt uitgevoerd alsmede de wijze waarop de naleving van de privacy wet- en regelgeving en de wijze waarop de uitvoering van de rechten van betrokkene plaatsvindt, moeten binnen de organisatie worden vastgelegd. Hiermee krijgt de organisatie de beschikking over standaard procedures, protocollen en formulieren waarmee de implementatie, naleving en inbedding in de organisatie kunnen worden uitgevoerd, gewaarborgd en bewerkstelligd.

Raadsnota

3. Relatie met bestaand beleid

Binnen de gemeente Maastricht is een, telkens groeiend, aantal verwerkingen van persoonsgegevens geconformeerd aan de Wet bescherming persoonsgegevens.
Het privacybeleid binnen de gemeente Maastricht krijgt met de verordening een formeel karakter. Deze verordening zorgt ook voor een juridische basis voor het openbare register van verwerkingen van persoonsgegevens.

4. Voorstel

Voorgesteld wordt de Privacyverordening Gemeente Maastricht vast te stellen.
Op deze manier krijgt het privacybeleid een formeel karakter; de organisatie krijgt de beschikking over standaard procedures, protocollen en formulleren waarmee de implementatie, naleving en inbedding in de organisatie kunnen worden uitgevoerd, gewaarborgd en bewerkstelligd.

Burgemeester en Wethouders van Maastricht,

De Secretaris, De Burgemeester,

Drs. J.D. Nauta. Drs. G. Leers.

DE RAAD DER GEMEENTE MAASTRICHT,

gezien het voorstel van Burgemeester en Wethouders d.d. 27 januari 2009, domein PID, no. 2009.01343;

gehoord de commissie Algemene Zaken, Openbare Orde en Veiligheid

BESLUIT:

PRIVACYVERORDENING GEMEENTE MAASTRICHT

Waar in de verordening de mannelijke persoonsvorm wordt gebruikt moet tevens de vrouwelijke persoonsvorm worden gelezen.

Afdeling 1 Begripsomschrijvingen en toepassingsgebied

Artikel 1 Begripsomschrijvingen
In aansluiting bij en in aanvulling op de Wet bescherming persoonsgegevens (Stb. 2000, nr. 302) wordt in deze Verordening en de daarop berustende bepalingen verstaan onder:
a. de wet: Wet bescherming persoonsgegevens (Wbp);
b. verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens;
c. verantwoordelijke: het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
d. bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreekse gezag te zijn onderworpen;
e. College bescherming persoonsgegevens: het toezichthoudend orgaan als bedoeld in hoofdstuk 9, paragraaf 1 van de wet;
f. betrokkene: degene op wie een persoonsgegeven betrekking heeft en die uit dien hoofde het recht heeft de eigen gegevens in te zien, deze zo nodig te corrigeren en het recht bezwaar aan te tekenen tegen de verwerking van gegevens;
g. ontvanger: degene aan wie de persoonsgegevens worden verstrekt;
h. domeinen: de organisatorische eenheden van de gemeente Maastricht.

Artikel 2 Reikwijdte van de verordening
Deze verordening is van toepassing op alle verwerkingen van persoonsgegevens die plaatsvinden binnen de domeinen en die vallen onder de werkingssfeer van de wet.

Afdeling 2 Uitgangspunt voor een goede gegevensverwerking

Artikel 3 Algemene beginselen
1. Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

2. Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld.
3. Persoonsgegevens worden slechts verwerkt indien daarvoor op grond van artikel 8 van de wet een rechtmatige grondslag aanwezig is.
4. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
5. Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.
6. Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.
7. De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in de wet. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Artikel 4 Geheimhoudingsplicht
1. Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker alsmede de bewerker zelf, voor zover deze toegang heeft tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen.
2. De personen, bedoeld in het eerste lid, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens, waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit. Artikel 272, tweede lid, van het Wetboek van strafrecht is niet van toepassing.

Artikel 5 Beveiliging
1. De verantwoordelijke zorgt voor een passende beveiliging van persoonsgegevens door middel van het hebben, onderhouden en naleven van een gemeentebreed informatiebeveiligingsbeleid conform de Code voor Informatiebeveiliging. Deze maatregelen garanderen een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich mee brengen. De verantwoordelijke ziet toe op de naleving van die maatregelen.
2. In het informatiebeveiligingsbeleid is vastgelegd:
a. wie op directieniveau eindverantwoordelijk is voor gemeentebrede informatiebeveiliging, waaronder de beveiliging van persoonsgegevens;
b. dat een stuurgroep informatiebeveiliging de eindverantwoordelijke voor de gemeentebrede informatiebeveiliging adviseert;
c. hoe de informatiebeveiligingsorganisatie verder is ingevuld;
d. hoe de bekostiging van de informatiebeveiliging is geregeld;
e. hoe de planning en control van de gemeentebrede informatiebeveiliging is geregeld.
3. De functionaris gegevensbescherming maakt deel uit van de stuurgroep die de eindverantwoordelijke voor de gemeentebrede informatiebeveiliging adviseert.

4. De uitvoering van de verwerkingen door de bewerker wordt geregeld in een schriftelijke overeenkomst of krachtens een andere schriftelijke rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en verantwoordelijke.

Afdeling 3 Verantwoordelijke en toezicht

Artikel 6 Verantwoordelijke
1. Het college van burgemeester en wethouders is de verantwoordelijke voor de verwerking van persoonsgegevens.
2. De verantwoordelijke benoemt per domein de teammanagers als beheerder en mandateert deze om namens hem de nodige stappen te nemen teneinde te voldoen aan de verplichtingen van de wet.

Artikel 7 Functionaris voor de gegevensbescherming (interne toezichthouder op een rechtmatige verwerking van persoonsgegevens)
1. Het college van burgemeester en wethouders benoemt een functionaris voor de gegevensbescherming die belast is met het toezicht op het privacy- en informatiebeveiligingsbeleid van de gemeente Maastricht.
2. Tot de taken van de functionaris voor de gegevensbescherming behoren in elk geval:
a. het zijn van aanspreekpunt voor alle zaken de bescherming van de persoonlijke levenssfeer betreffende;
b. het informeren en adviseren van de contactpersonen die worden genoemd in het openbaar register betreffende de verwerking van persoonsgegevens omtrent privacy- en beveiligingsbeleid;
c. het organiseren van activiteiten die een voortdurende bewustwording ten aanzien van de gegevensbescherming ten doel hebben;
d. het beheer van en de verantwoordelijkheid voor het openbaar register,waarin alle verwerkingen van persoonsgegevens die plaatsvinden binnen de gemeente Maastricht worden opgenomen.
e. het onderhouden en aanvullen van het openbaar register met alle verwerkingen die binnen de te onderscheiden domeinen zijn geïnventariseerd;
f. het beoordelen van nieuwe of aangepaste verwerkingen in het licht van de meldingsplicht en andere verplichtingen;
g. het in opdracht van en met goedkeuring van de directeur van de te onderscheiden domeinen ontwikkelen van een privacybeleid voor het betreffende domein;
h. het communiceren met de directeur en de medewerkers van het domein over alle ontwikkelingen op het gebied van techniek en wetgeving die relevant zijn voor het privacy- en beveiligingsbeleid van dat domein;
i. uitwisselen van ervaring met betrekking tot de wet en andere relevante wet- en regelgeving.

Afdeling 4 Inschrijving van de verwerkingen in een "openbaar register"

Artikel 8 Het openbaar register
1. Het college van burgemeester en wethouders houdt een openbaar register, bestemd voor de inschrijving van verwerkingen van persoonsgegevens, waarop deze verordening van toepassing is.
2. Bij die inschrijving worden in ieder geval de volgende gegevens vermeld:
a. de naam van de verwerking;

b. het beheer van de verwerking;
c. de doeleinden van de verwerking;
d. de personen van wie persoonsgegevens worden verwerkt(betrokkenen);
e. de persoonsgegevens die bij de verwerking worden gebruikt;
f. de ontvangers van de gegevens;
g. eventuele verstrekkingen aan andere landen buiten de Europese Unie;
h. de bewaartermijnen die in acht genomen worden en
i. eventuele bijzonderheden.
3. Het college van burgemeester en wethouders besluit tot doorhaling van de inschrijving van een verwerking in het register indien de verwerking wordt opgeheven.

Artikel 9 Nadere regels
Het college van burgemeester en wethouders kan nadere regels stellen, waarin is vastgelegd:
a. hoe uitvoering wordt gegeven aan de inschrijving van een verwerking van persoonsgegevens in het register en de doorhaling van een inschrijving, alsmede aan het aanbrengen van wijzigingen in de gegevens die omtrent een verwerking in het register zijn vastgelegd;
b. welke informatie het register over elke ingeschreven persoonsregistratie moet bevatten en op wie de verplichting tot het tijdig aanleveren van deze informatie rust en
c. hoe aan de openbaarheid van het register gestalte wordt gegeven.

Afdeling 5 Informatieplicht en toegang tot het openbaar register

Artikel 10 Informatieplicht
1. De verantwoordelijke deelt de betrokkene op het moment van vastlegging van hem betreffende gegevens mede wat de identiteit is van de verantwoordelijke en de doeleinden van de verwerking.
2. De informatieplicht geldt niet wanneer de betrokkene uit andere hoofde reeds op de hoogte is.
3. Het eerste lid is niet van toepassing indien mededeling van de informatie aan betrokkene onmogelijk blijkt of een onevenredige inspanning kost.
4. Het openbaar register vormt een middel om te voldoen aan de informatieplicht.

Artikel 11 Toegang tot het openbaar register
De verantwoordelijke verleent een ieder die daarom verzoekt toegang tot de informatie opgenomen in het openbaar register.

Artikel 12 Recht op inzage en kennisgeving en verstrekking
1. De betrokkene heeft het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De verantwoordelijke stuurt het verzoek door aan de daartoe ter behandeling aangewezen functionaris gegevensbescherming dan wel de eveneens daartoe ter behandeling aangewezen betrokken teammanager, deze vergewist zich van de identiteit van de verzoeker. De functionaris gegevensbescherming of de

betrokken teammanager deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt.
2. Indien zodanige gegevens worden verwerkt, bevat de mededeling een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van het doel of de doeleinden van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën van ontvangers, alsmede de beschikbare informatie over de herkomst van de gegevens.
3. Voordat de functionaris gegevensbescherming of de betrokken teammanager een mededeling doet als bedoeld in het tweede lid, waartegen een derde naar verwachting bedenkingen zal hebben, stelt hij die derde in staat zijn zienswijze naar voren te brengen, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost.
4. Indien een gewichtig belang van de verzoeker dit eist voldoet de functionaris gegevensbescherming of de betrokken teammanager aan het verzoek in een andere dan schriftelijke vorm, die aan dat belang is aangepast.
5. Een verzoek wordt ten aanzien van minderjarigen die de leeftijd van zestien jaren nog niet hebben bereikt, en ten aanzien van onder curatele gestelde gedaan door hun wettelijke vertegenwoordigers. De betrokken mededeling geschiedt eveneens aan de wettelijke vertegenwoordigers.

Artikel 13 Recht op correctie, aanvulling en verwijdering
1. De door de verantwoordelijke daartoe aangewezen functionaris gegevensbescherming dan wel de eveneens daartoe aangewezen betrokken teammanager zal op schriftelijk verzoek van een betrokkene de met betrekking tot deze persoon te verwerken persoonsgegevens verbeteren, aanvullen of verwijderen, indien deze feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek behelst de aan te brengen wijzigingen.
2. De functionaris gegevensbescherming of de betrokken teammanager bericht de verzoeker zo spoedig mogelijk doch uiterlijk binnen vier weken na ontvangst van het verzoek schriftelijk of, dan wel in hoeverre, hij daaraan voldoet. Een weigering is met redenen omkleed.
3. De functionaris gegevensbescherming of de betrokken teammanager zorgt er voor dat een beslissing tot verbetering, aanvulling of verwijdering zo spoedig mogelijk wordt uitgevoerd.
4. De functionaris gegevensbescherming of de betrokken teammanager die aan een verzoek tot verbetering, aanvulling of verwijdering voldoet zal degenen aan wie hij naar zijn weten in het jaar voorafgaand aan het verzoek en in de sinds dat verzoek verstreken periode de betrokken gegevens heeft verstrekt hiervan mededeling doen tenzij de verzoeker te kennen heeft gegeven hierop geen prijs te stellen. De functionaris gegevensbescherming of de betrokken teammanager doet aan de verzoeker opgave van degenen aan wie hij de mededeling heeft gedaan.
5. Een verzoek wordt ten aanzien van minderjarigen die de leeftijd van zestien jaren nog niet hebben bereikt, en ten aanzien van onder curatele gestelde gedaan door hun wettelijke vertegenwoordigers. De betrokken mededeling geschiedt eveneens aan de wettelijke vertegenwoordigers.

Artikel 14 Recht van verzet
1. Indien gegevens het voorwerp zijn van verwerking op grond van artikel 8, onder e en f, van de wet, kan de betrokkene bij de verantwoordelijke te allen tijde bezwaar aantekenen tegen verwerking van zijn persoonsgegevens in verband met zijn bijzondere persoonlijke omstandigheden.

2. Binnen vier weken na ontvangst van het verzet beoordeelt de door de verantwoordelijke daartoe aangewezen functionaris gegevensbescherming dan wel de eveneens daartoe aangewezen betrokken teammanager of dat verzet gerechtvaardigd is.
3. Indien een dergelijk verzet gerechtvaardigd is of indien verzet is aangetekend tegen verwerking voor commerciële of charitatieve doeleinden treft de functionaris gegevensbescherming of de betrokken teammanager in dat geval maatregelen om deze vorm van verwerking terstond te beëindigen.

Afdeling 6 Slotbepalingen

Artikel 15 Onvoorziene omstandigheden
In de gevallen waarin het bij of krachtens de wet dan wel deze verordening bepaalde niet voorziet of daaromtrent onduidelijkheid bestaat beslist het college van burgemeester en wethouders.

Artikel 16 Citeertitel en inwerkingtreding
1. Deze verordening kan worden aangehaald als: Privacyverordening gemeente Maastricht.
2. Deze verordening treedt in werking op de dag nadat deze is bekendgemaakt.

Aldus besloten door de raad der gemeente Maastricht in zijn openbare vergadering van 17 februari 2009.

De Griffier,

Drs. J.D. Nauta.

De Voorzitter,

Drs. G. Leers.