MILL EN ST.HUBERT

GEMEENTEBLAD

Officiële uitgave van de gemeente Mill en Sint Hubert

Nr. 39457

13 maart

2017

Privacy

Privacy is een onderwerp dat in de huidige (digitale) samenleving enorm in de belangstelling staat. Privacy is een ruim begrip: het gaat onder meer om de bescherming van persoonsgegevens, de bescherming van het eigen lichaam en van de eigen woning, de bescherming van familie- en gezinsleven, en het recht vertrouwelijk te communiceren via, brief, telefoon, e-mail en dergelijke.

Privacy is samenvattend te omschrijven als "*respect voor de persoonlijke levenssfeer van een individu*".

Dit respect dient niet alleen in acht te worden genomen door de overheid maar geldt voor iedereen dus ook voor bijvoorbeeld bedrijven en burgers onderling. De eerbiediging van de persoonlijke levenssfeer, is als grondrecht opgenomen in artikel 10 van de Grondwet. Om te voorkomen dat een onnodige of te vergaande inbreuk wordt gemaakt op de persoonlijke levenssfeer, is voorzien in (wettelijke) waarborgen. Privacyregels dienen te voorkomen dat, onder andere, de overheid zich onnodig mengt in het persoonlijke leven van burgers. Daarnaast eisen deze regels dat de overheid zorgvuldig omgaat met de persoonlijke informatie waarover zij beschikt.

Persoonsgegevens

Om haar taken te kunnen uitvoeren, verzamelt en verwerkt elke gemeente persoonsgegevens. De verwerking van persoonsgegevens is daarmee inherent aan de gemeentelijke taakuitoefening. Met de overdracht van taken in het sociaal domein heeft een gemeente (nog) meer privacygevoelige gegevens te verwerken gekregen. De complexiteit in het kader van de bescherming van persoonsgegevens is toegenomen. Nog meer dan voorheen, doen burgers een beroep op ondersteuning en/of hulp door de gemeente. De gemeente zal door deze taakuitbreiding, vaker dan voor de decentralisaties het geval was, persoonsgegevens uitwisselen met instanties buiten de gemeentelijke organisatie. Informatieverwerking gaat gepaard met de verantwoordelijkheid om effectieve privacybescherming te bieden.

Daarnaast wordt de bescherming van persoonlijke gegevens steeds complexer. Zwakke beveiliging en/of niet adequate verwerking van persoonsgegevens kan leiden tot onacceptabele situaties waarbij bijvoorbeeld iemands identiteit wordt gestolen en misbruikt. De Autoriteit Persoonsgegevens (voorheen het College bescherming persoonsgegevens) streeft voortdurend naar een behoorlijke en zorgvuldige verwerking van persoonsgegevens door, onder andere, gemeenten. Vanaf 1 januari 2016 heeft de Autoriteit Persoonsgegevens (hierna "AP") meer en zwaardere bevoegdheden gekregen om te handhaven tegen de overtredingen van de Wet bescherming persoonsgegevens (hierna Wbp). Daarnaast is vanaf dat moment de Wet meldplicht datalekken ingevoerd.

De AP kan nu boetes opleggen en organisaties zijn verplicht om ernstige datalekken te melden aan de AP.

Beleid en reglement

Het op een juiste wijze verzamelen en verwerken van privacygevoelige informatie en de bescherming van deze gegevens, is dan ook een zeer relevant onderwerp voor de gemeenten Cuijk, Grave, Mill en Sint Hubert. De colleges van deze gemeenten zijn verantwoordelijk voor de verwerking van de persoonsgegevens die bij de gemeenten aanwezig zijn. Het college is de "*verantwoordelijke*" zoals bedoeld in artikel 1 onder d van de Wbp.[1] Het college blijft ook de verantwoordelijke op het moment dat de gegevens ter beschikking worden gesteld aan een derde of worden gedeeld in een samenwerkingsverband.

Door de samenwerking binnen de Werkorganisatie CGM (hierna "de Werkorganisatie") is er een bijzondere constructie van kracht. Hoewel het college van elke deelnemende gemeente wordt aangemerkt als "*verantwoordelijke*", zijn de medewerkers die de gegevens daadwerkelijk verwerken, in dienst van de Werkorganisatie. Daarnaast is de Werkorganisatie als bestuursorgaan tevens verantwoordelijk voor de verwerking van de gegevens zoals die binnen CGM plaatsvindt. Denk hierbij aan de verwerking van de salarisadministratie. Ook voert de Werkorganisatie onder andere, samen met het Basisteam Centrum Jeugd en Gezin Land van Cuijk en diverse ketenpartners, de werkzaamheden in het kader van de

1) *Verantwoordelijke:* de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1 onder "d" Wbp)

Jeugdwet uit. De Werkorganisatie verricht deze taken in opdracht van de gemeente Cuijk omdat Cuijk, door de andere 4 gemeenten in het Land van Cuijk, als centrumgemeente voor deze werkzaamheden is aangewezen.

De gemeenten Cuijk, Grave en Mill en Sint Hubert alsmede de Werkorganisatie hechten er veel waarde aan dat de verwerkingen van persoonsgegevens zorgvuldig, rechtmatig en veilig plaatsvinden. Het zorgvuldig omgaan met gegevens vormt een essentiële bouwsteen voor het vertrouwen in de gemeenten, in de Werkorganisatie en in de samenwerkingsverbanden waarin de gemeenten en de Werkorganisatie deelnemen.

Naleving van wet- en regelgeving op het gebied van de privacybescherming vormt het uitgangspunt van handelen bij de uitvoering van de primaire processen en de bedrijfsvoering en wordt opgevat als kenmerk van goede dienstverlening en de daarbij behorende kwaliteit. Hoewel de wettelijke uitgangspunten dus in acht worden genomen, gaat de Wbp echter ook uit van zelfregulering en is er soms ruimte voor interpretatie.

De colleges van burgemeester en wethouders en het bestuur van de Werkorganisatie hebben daarom besloten eenduidig een algemeen beleid te formuleren hoe om te gaan met het verwerken van persoonsgegevens. In dit beleid staan de uitgangspunten beschreven voor het verwerken van persoonsgegevens, de bescherming van en de omgang met deze gegevens. Deze uitgangspunten zijn vervolgens juridisch vertaald in een reglement.

Doel

Het doel van het beleid en het reglement is het bieden van algemene richtlijnen om de persoonsgegevens zorgvuldig, doelmatig en veilig te verwerken. Daarnaast dient er overzicht en inzicht te worden verkregen en te worden behouden met betrekking tot het verwerken van de persoonsgegevens ook wanneer de verwerking wordt uitgevoerd door een derde partij. De documenten bieden regels om te communiceren over de verwerking van de persoonsgegevens en zorgen ervoor dat de rechten van betrokkenen inzichtelijk zijn en worden nageleefd.

Vaak wordt alleen een beleid en/of reglement gemaakt voor het sociaal domein. Persoonsgegevens worden echter door bijna alle medewerkers verwerkt. De colleges en het bestuur zijn daarom van mening, dat er een algemeen organisatiebreed beleid en reglement dient te zijn dat op de gehele organisatie van toepassing is.

Hierin wordt door dit beleid en het bijbehorende reglement voorzien. Tevens is het, gelet op de nauwe verwevenheid van "*privacy*" met de onderwerpen "*integriteit*" en "*informatiebeveiliging*" van belang dat (aandacht voor) privacybescherming binnen de gehele organisatie wordt ingevoerd.

Het is soms noodzakelijk dat voor sommige gegevens extra voorwaarden en/of maatregelen worden gesteld. In die gevallen zijn de algemene regels niet voldoende en dient er te worden voorzien in maatwerk. Zo gelden er bijvoorbeeld specifieke/aanvullende regels voor Suwinet. Gelet op de bevoegdheidsverdeling kan het dan zo zijn, dat deze aanvullende regels alleen door de colleges worden vastgesteld. Deze systematiek loopt parallel met het informatiebeveiligingsbeleid: er wordt uitgegaan van een algemene basis (de Baseline Informatiebeveiliging Gemeenten), als specifieke wetgeving dit vereist, dient deze basis te worden aangevuld. De benodigde aanvullende maatregelen worden vastgesteld door het daartoe bevoegde bestuursorgaan.

Op korte termijn wordt voorzien in een privacyprotocol voor het Basisteam Centrum Jeugd en Gezin Land van Cuijk en voor de sociale kernteams. In deze protocollen worden de regels van het algemene beleid en reglement als basis ("*kapstok*') gehanteerd en waar nodig zijn deze voorschriften aangepast aan de specifieke situatie. Ook voor toekomstige ontwikkelingen, denk hierbij aan samenwerkingsvormen of (tijdelijke) projecten waarbij gegevens worden uitgewisseld, dienen het algemene privacybeleid en –reglement als uitgangspunt te worden genomen.

Reikwijdte

De kaders zoals die in dit beleid en het reglement worden gesteld, gelden voor de (medewerkers van) de gemeenten en de Werkorganisatie maar ook voor samenwerkingsverbanden die zijn of worden aangegaan en derden die zijn of worden ingeschakeld om gegevens te verwerken.

Het beleid en het reglement zijn van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens binnen de administratieve en bestuurlijke organisatie waarop de Wbp van toepassing is en waarvoor het college of het bestuur van de Werkorganisatie "*verantwoordelijke*"

is. Daarnaast is het tevens van toepassing op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Wet bescherming persoonsgegevens

Bescherming van de persoonlijke levenssfeer is een grondrecht. Dit recht is geregeld in artikel 10 lid 1 van de Grondwet, artikel 8 van het Europees Verdrag inzake de rechten van de mens en de fundamentele vrijheden (EVRM) en artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR).

Deze 3 artikelen geven aan dat er een wet moet zijn voor de bescherming van persoonsgegevens zodat ieders recht op privacy is gewaarborgd. In Nederland is dit de Wbp. De Wbp is sinds 1 september 2001 van kracht en vormt een kaderwet waaraan publieke en private organisaties zich moeten houden.

Bij gegevensbescherming gaat het om het zorgvuldig, veilig en doelmatig verwerken van persoonsgegevens.

Met "*verwerken*" wordt bedoeld: alle handelingen die een organisatie kan uitvoeren met persoonsgegevens. Dit is dus een zeer ruim begrip. Handelingen die er volgens de Wbp in ieder geval onder vallen, zijn: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.[2]

Volgens de Wbp is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon een persoonsgegeven.[3] Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn. Er zijn vele soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden ook wel "*bijzondere persoonsgegevens*" genoemd.[4] Deze zijn door de wetgever extra beschermd.

De "*verantwoordelijke*" is een persoon of een organisatie die het doel van en de middelen voor het gebruik van persoonsgegevens bepaalt.[5] Dit houdt in dat de verantwoordelijke uiteindelijk beslist of een organisatie persoonsgegevens verwerkt en indien tot verwerken wordt overgegaan, om welke verwerking het gaat, welke persoonsgegevens de organisatie hierbij verwerkt, voor welk doel de organisatie dit doet en op welke manier de organisatie dit doet.

De "*betrokkene*" is degene van wie een organisatie persoonsgegevens verwerkt.[6] Dit is dus degene op wie de persoonsgegevens betrekking hebben.

Een "*bewerker*" is een persoon of organisatie aan wie de verantwoordelijke de gegevensverwerking heeft uitbesteed.[7] Een bewerker is niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens. Maar de bewerker heeft wel een aantal afgeleide verplichtingen, voor onder meer beveiliging en geheimhouding van de gegevens.

2) artikel 1 onder "b" Wbp

3) artikel 1 onder "a" Wbp

4) paragraaf 2 (artikel 16 en verder) Wbp

5) artikel 1 onder "d" Wbp

6) artikel 1 onder "f" Wbp

7) artikel 1 onder "e" Wbp

Bewerkersovereenkomst

Bij veel processen worden gegevens verwerkt door "*bewerkers*". Hierbij kan men denken aan een applicatie waarbij persoonsgegevens buiten het bereik van de gemeenten en/of de Werkorganisatie door een leverancier worden verwerkt.

Het uitbesteden van werkzaamheden aan deze derden brengt risico's met zich mee op het gebied van gegevensverwerking en informatiebeveiliging. Het college van burgemeester en wethouders of het bestuur van de Werkorganisatie blijven verantwoordelijk voor de verwerking van de gegevens. Zij moeten er daarom op toezien dat gegevens juist verwerkt en beveiligd worden.[8] Hiervoor dienen bewerkersovereenkomsten te worden gesloten. In deze overeenkomst wordt onder andere beschreven met welk doel de gegevens worden verstrekt en voor welke verwerking de informatie mag worden gebruikt maar tevens worden in een dergelijke overeenkomst eisen gesteld aan de beveiligingsmaatregelen die de bewerker in opdracht van de verantwoordelijke neemt.

De Wbp schrijft namelijk voor dat er passende technische en organisatorische beveiligingsmaatregelen getroffen worden om de gegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.[9] Op basis van de Wet meldplicht datalekken wordt van de verantwoordelijke verwacht dat hij overzicht en inzicht heeft in alle gegevensverwerkingen waar hij verantwoordelijk voor is.

Meldplicht datalekken

Vanaf 1 januari 2016 is de Wet meldplicht datalekken in werking getreden. Dit is een aanvulling op de Wbp en loopt vooruit op de Algemene Verordening Gegevensbescherming. Een datalek is een inbreuk op de beveiliging, waarbij een aanzienlijke kans bestaat dat dit ernstige gevolgen dan wel ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens heeft.[10] Hierbij kan gedacht worden aan het kwijtraken van een USB stick met persoonsgegevens, inbraak door een hacker, maar ook onbevoegde autorisaties in een informatiesysteem.

De verantwoordelijke is verplicht om ernstige datalekken te melden bij de AP. Het gaat hier om datalekken waar de gemeente of de werkorganisatie voor verantwoordelijk is. Daaronder vallen ook datalekken die ontstaan bij een derde partij die werkzaamheden uitvoert voor de gemeente en/of de Werkorganisatie vandaar dat de hiervoor genoemde bewerkersovereenkomsten hierbij een belangrijke rol spelen.

Algemene Verordening Gegevensbescherming

Op 25 mei 2016 is de (Europese) Algemene Verordening Gegevensbescherming (hierna AVG) in werking getreden. Deze nieuwe wetgeving moet zorgen voor harmonisatie van de huidige privacyregelgeving in Europa en verbetering van de privacy(bescherming) van burgers. De oude privacyregelgeving (1995) werd vastgesteld toen internet nog in de kinderschoenen stond. Bij de nieuwe regelgeving gaat het daarom vooral om het beschermen van persoonsgegevens in de digitale wereld. De Europese Unie wil met de AVG het vertrouwen bij burgers en consumenten in de verwerking van persoonsgegevens door overheid en bedrijven vergroten.

Deze (Europese) verordening heeft een directe werking en hoeft niet meer in nationale wetgeving geïmplementeerd te worden. Dat betekent dat het privacy beleid straks rechtstreeks aan deze verordening dient te voldoen. Alle organisaties in de publieke en private sector hebben 2 jaar (dus tot 25 mei 2018) de tijd om aan de nieuwe wetgeving te voldoen.

De belangrijkste verandering wordt dat de nieuwe Europese wetgeving tot het opleggen van 1 of meer bestuurlijke boete(s) kan leiden, die zal worden opgelegd door de AP als de verordening niet wordt

8) artikel 14 Wbp

9) artikel 14 Wbp

10)artikel 34a Wbp

nageleefd. Verder is de verordening een antwoord op de nieuwe mogelijkheden en uitdagingen die ontwikkelingen in ICT met zich meebrengen, bijvoorbeeld met het recht om te worden vergeten.

De insteek van de verordening verlegt de focus van een externe meldplicht (die in de huidige wetgeving zit) vooral naar een eigen verantwoordelijkheid van organisaties om intern risico beperkende maatregelen te nemen zoals het uitvoeren van Privacy Impact Assessments, het hanteren van privacy bij design en het benoemen van een functionaris voor de gegevens bescherming. De aanwijzing van een functionaris voor de gegevensbescherming is niet langer vrijblijvend, maar wordt verplicht voor organisaties die veel persoonsgegevens verwerken zoals gemeenten.

Informatieveiligheid

Artikel 13 van de Wbp vormt het algemeen wettelijk kader voor de beveiliging van persoonsgegevens. Op basis van dat artikel dient de verantwoordelijke de noodzakelijke beveiligingsmaatregelen te treffen ter voorkoming van misbruik en verlies van persoonsgegevens. Gegevensbescherming kan alleen gerealiseerd worden door borging van de informatieveiligheid. Voor de informatieveiligheid zijn binnen de gemeenten en de Werkorganisatie de kaders van de Strategische en Tactische Baseline Informatievoorziening Gemeenten (BIG) van toepassing.

Naleving van de BIG zorgt daarmee voor meer informatieveiligheid die een eerste voorwaarde is voor gegevensbescherming in het kader van privacy.

De (verdere) ontwikkeling van het veiligheidsbeleid loopt daardoor parallel met de (door) ontwikkeling van het privacybeleid. Waar privacybeleid met name gaat over *hoe* om te gaan met persoonsgegevens, gaat het beveiligingsbeleid over de strategische, tactische en operationele maatregelen die worden getroffen om de persoonsgegevens te beveiligen. Privacy, informatieveiligheid en integriteit vormen 3 onderwerpen die onlosmakelijk met elkaar verbonden zijn en die dan ook in onderlinge samenhang geborgd moeten worden.

Borging

De wijze waarop het privacy- en het informatiebeveiligingsbeleid binnen de 3 gemeenten en de Werkorganisatie wordt verankerd, vorm het fundament van de privacy borging. De colleges en het bestuur zijn verantwoordelijk voor juiste gegevensverwerking en informatiebeveiliging. Echter, deze verantwoordelijkheid beperkt zich niet alleen tot het bestuur of het college. Zorgvuldige gegevensverwerking geldt voor iedereen die binnen de gemeente en/of de Werkorganisatie werkzaam is. Het gaat daarbij niet alleen om bestuurders en medewerkers met een dienstverband, maar bijvoorbeeld ook om ingehuurde medewerkers of adviseurs.

Gegevensbescherming wordt niet alleen geborgd door het uitvoeren van analyses, checklists en het nemen van maatregelen. Het is ook van belang dat er bewust, integer en informatieveilig met persoonsgegevens wordt omgegaan. Om deze bewustwording te realiseren is, onder andere, kennisoverdracht nodig. In het kader van de 3 genoemde aandachtsgebieden: privacy, integriteit en informatieveiligheid worden de rollen en verantwoordelijkheden met betrekking tot deze onderwerpen herhaaldelijk onder de aandacht gebracht van bestuurders, management en medewerkers. In het uiterste geval kan het niet in acht nemen van privacy-, integriteits- of informatiebeveiligingsnormen of ernstige schending daarvan leiden tot het nemen van sanctiemaatregelen.

Zoals aangegeven, is er een sterkte verwantschap met het informatiebeveiligingsbeleid en de daaruit voortvloeiende documenten. Zonder een goede informatiebeveiliging, is het niet mogelijk om te garanderen dat gegevens goed worden beschermd. Informatiebeveiliging is, net als privacy, een *"dynamisch"* onderwerp. Deze dynamiek heeft niet alleen te maken met ontwikkelingen die zich momenteel in snel tempo opvolgen en waar voortdurend op ingespeeld moet worden, maar tevens met het feit dat er, relatief gezien, nog maar net gestart is met de implementatie van deze beide onderwerpen voor de Werkorganisatie en de deelnemende gemeenten.

Looptijd en evaluatie

Zoals hiervoor beschreven is privacy, mede in relatie met informatiebeveiliging, zeker op dit moment een dynamisch onderwerp. De ontwikkelingen volgen zich in snel tempo op. Dit heeft niet alleen te maken dat de kaders voor de gegevensverwerking binnen het sociaal domein steeds beter vorm krijgen, ook de Europese ontwikkelingen zoals het in werking treden van de AVG brengen de nodige wijzigingen met zich mee.

De houdbaarheid van het onderhavige beleid en het bijbehorende reglement is op dit moment moeilijk te voorspellen maar gelet op de aanpassingen die voort gaan vloeien uit de AVG (zoals de verplichte aanstelling van een functionaris voor de gegevensbescherming) zullen er toe leiden dat het beleid en het reglement hoogstwaarschijnlijk niet erg lang in stand kunnen blijven en voor 25 mei 2018 moeten worden herzien.

Om, ondanks de ontwikkelingen die nu reeds voorzien worden, op dit moment toch een kader met betrekking tot gegevensbescherming te bieden, is het voorliggende beleid met het bijbehorende reglement opgesteld. Voorgesteld wordt, op het moment dat aanpassing van het algemene beleid en reglement noodzakelijk is, niet alleen de benodigde aanpassingen door te voeren, maar tevens het beleid en het reglement te evalueren en te bekijken of aanpassing, gelet op de werking in de dagelijkse praktijk, noodzakelijk is.

Reeds enkele malen is in dit beleid een koppeling gelegd tussen dit beleid en het informatiebeveiligingsbeleid (en de daaruit voortvloeiende plannen en regels) en het onderwerp "*integriteit*". Met name voor informatieveiligheid geldt, dat ook hier sprake is van een onderwerp dat voortdurend aandacht en aanpassing vraagt, zeker omdat hierbij sprake is met een nauwe verwevenheid van gegevensbescherming met het oog op privacy. Technische ontwikkelingen zoals bijvoorbeeld cryptoware vragen een continue alertheid. Dit maakt dat een strikte scheiding tussen (maatregelen op het gebied van) privacy en informatiebeveiliging ook niet altijd mogelijk is. Dit is echter ook niet nodig want "*informatieveiligheid, privacy en integriteit: samen vormen ze een driehoek waar elke ambtenaar elke dag mee bezig moet zijn*".[11] Voorgesteld wordt om deze stelling als leidraad te nemen voor de inrichting van deze driehoek voor de komende periode.

11)Citaat van Frans Backhuis, burgemeester van Nieuwegein en voorzitter van de Visitatiecommissie Informatieveiligheid van de VNG, website VNG (https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid-privacy/nieuws/een-driehoek-van-veiligheid) 4 oktober 2016