advies aan b&w

GEMEENTE WEERT

Sector	: Bedrijfsvoering	Openbaar: ☑
Afdeling	: Personeel, Informatie en Facilitair	Niet openbaar: ☐
Zaaknummer(s) ingekomen stuk(ken)	:	Kabinet: ☐
Behandelend medewerk(st)er	: Marco van Dijk Tel.: (0495) 57 55 82	
Portefeuillehouder(s)	: A.A.M.M. Heijmans	Nummer B&W-advies: BW-007966

ONDERWERP

Privacybeleid en stappenplan sociaal domein

ADVIES

- Besluiten tot vaststelling van de uitgangspunten integraal privacybeleid zoals neergelegd in bijgevoegde notitie
- Instemmen met het bijbehorende stappenplan privacybescherming voor het sociaal domein

TOELICHTING

[Invulinstructie]

Relatie met vorig voorstel:
N.v.t.

Algemeen:
Met ingang van 2015 heeft de gemeente belangrijke taken en verantwoordelijkheden ingevolge de Jeugdwet, de Participatiewet en de Wet maatschappelijke ondersteuning 2015.
De decentralisaties maken het voor de gemeente mogelijk om dienstverlening in het sociale domein aan burgers beter te organiseren. Daarbij gaat het er zowel om te zorgen voor een integrale dienstverlening aan de burger, als ook om een betere aanpak van multiprobleemsituaties. De decentralisaties en de beoogde integrale werkwijze van de gemeente brengt met zich mee dat de gemeente, meer dan voorheen, persoonsgegevens van burgers zal verwerken en hiervoor ook meer zal samenwerken met andere partners.

Weert, 21 januari 2015		S		B	W HL	W FvE	W PS	W GG
De directeur, 22/1/15			akkoord					
			bespreken					
		Behandeling uiterlijk in college van 27 januari 2015						

In te vullen door het B&W secretariaat:

☐ Akkoord
☐ Akkoord met tekstuele aanpassing door portefeuillehouder
☐ Anders, nl.:

☐ Niet akkoord
☐ Gewijzigde versie

☐ A-stuk
☐ B-stuk
☐ C-stuk

Beslissing d.d.: Akkoord met advies 27 JAN. 2015

Nummer: 4

De secretaris,

Totaal aantal pagina's: 3
Pagina 1

Argumenten:
Burgers moeten erop kunnen vertrouwen dat er zorgvuldig wordt omgegaan met persoonsgegevens wanneer zij bepaalde zorg of dienstverlening ontvangen. De wijze van gegevensverwerking is vastgelegd in de sectorwetgeving. Hierin zijn de wettelijke grondslagen vastgelegd op basis waarvan de gemeente gegevens kan verwerken. De gemeente staat voor de uitdaging om de wettelijke kaders toe te passen in de praktijk. Bij de toepassing van die kaders, en voor situaties waarin de sectorwetgeving geen specifieke aanvullende regels geven is de Wet bescherming persoonsgegevens (Wbp) leidend. In het algemeen roept de wbp op tot terughoudendheid bij gegevensverwerking. De Wbp dwingt tot zorgvuldige afwegingen met betrekking tot gegevensverwerking. De wettelijke kaders dienen als handvat, maar het formuleren van het privacybeleid is maatwerk, net als de implementatie en borging daarvan in de processen en systemen.

Het is belangrijk dat de gemeente een visie heeft op deze gegevensverwerking in relatie tot het waarborgen van de privacy van burgers. Daarnaast is het van belang dat de verantwoordelijkheden worden belegd. De wet wijst het college aan als probleemeigenaar van privacybeleidsvoering. Vanwege de noodzakelijke samenwerking met partners zal het college op haar beurt verantwoordelijkheden aan anderen moeten opdragen. Het maken van afspraken hieromtrent is dus noodzakelijk.

Binnen de gemeente is m.b.t. privacy op thematisch gebied en op gebied van informatiebeveiliging al veel geregeld. Om hier zicht op te krijgen is onlangs een zogenaamde Privacy Scan ingevuld. Op basis van deze scan, die door de projectgroep is voorgelegd aan het Ondersteuningteam Decentralisaties , wordt inzicht verkregen in wat al is geregeld en wat nog aandacht en actie vraagt. De huidige decentralisaties vragen, ook vanuit de wetgeving, als eerste om een samenhangend integraal beleid, dat als kapstok dient voor de verdere uitwerking binnen de gemeentelijke processen en de samenhang met samenwerkende partijen.

Bijgevoegde notitie bevat beleidsuitgangspunten op privacy alsmede een stappenplan voor de verdere optimalisering van privacybeleid tot het wettelijk niveau. Instemming met deze notitie bewijst direct good governance en biedt een eerste bescherming tegen bestuurdersaansprakelijkheid. Vooruitlopend op de totstandkoming van het integrale beleid en het thematisch beleid is het wenselijk dat met de geformuleerde uitgangspunten alsmede met het stappenplan wordt ingestemd

Risicoparagraaf

Privacybeleid dient binnen de gemeente te worden gekenmerkt door vanzelfsprekendheid en natuurlijke samenwerking. Optimalisering van beheersmaatregelen is een continu proces en gebeurt op basis van feedback en evaluaties. Handelen in afwijking van privacyregelgeving betekent dat het verwerken van persoonsgegevens onrechtmatig is. In praktische zin gaat dit om activiteiten zoals dossiervorming, casusoverleg, collegebesluiten en berichtenverkeer met bijvoorbeeld zorgaanbieders. Niet voldoen maakt het college kwetsbaar voor discussie en aansprakelijkheid. Iedere benadeelde kan dan aanspraak maken op schadevergoeding. De landelijk toezichthouder, het College Bescherming persoonsgegevens (CBP) kan op ieder moment een onderzoek instellen en dwangsommen/bestuurlijke boetes opleggen. In paragraaf 2.4 van de uitgangspuntennotitie wordt hierop nader ingegaan.

Kanttekeningen:
N.v.t.

JURIDISCHE GEVOLGEN (o.a. FATALE TERMIJNEN/HANDHAVING)
[Invulinstructie]

Gemeentelijke privacybeleid is een wettelijke verplichting. Ontoereikend opgesteld en ingevoerd beleid kan leiden tot claims, opgelegde boetes en imagoschade. Zie de risicoparagraaf.

FINANCIËLE EN PERSONELE GEVOLGEN

[Invulinstructie]

Begrotingspost:
Uitgangspunt is dat het stappenplan met de bestaande middelen wordt uitgevoerd. Het ontwikkelen van het privacybeleid aan de hand van het stappenplan wordt ondersteund vanuit de regionale samenwerking decentralisaties. Het uitwerken van het stappenplan zal verder vorm krijgen in een regionale werkgroep, bemenst vanuit de gemeenten met functionarissen uit de staande organisatie.
Het resultaat van het stappenplan is een bijgesteld privacybeleid dat voldoet aan de wettelijke maatstaven. Op dit moment is nog niet aan te geven of en in welke mate extra middelen nodig zijn voor implementatie van het privacybeleid.

Beschikbaar bedrag:
N.v.t.

COMMUNICATIE/PARTICIPATIE

Voor wie is dit advies van belang?:
- ❖ Interne organisatie
- ❖ Overigen (bijv. afzender/aanvrager)

Nadere specificatie: Op grond van het bepaalde in afdeling 3.6 van de Algemene wet bestuursrecht dient de beleidsnotitie te worden bekend gemaakt.

Geadviseerd wordt de volgende communicatie-instrumenten te gebruiken:
- ❖ Overig

Nadere specificatie:

Geadviseerd wordt de volgende participatie-instrumenten te gebruiken:
- ❖ Niet van toepassing

OVERLEG GEVOERD MET

[Invulinstructie]

Intern:
Juridisch medewerkers Sector Inwoners / Transitiemanager 3D.

Extern:
Notitie is tot stand gekomen in de regionale juridische werkgroep 3D.

BIJLAGEN

Openbaar:
Notitie 'Uitgangspunten en stappenplan integraal privacybeleid'

Niet-openbaar:
Niet van toepassing

Uitgangspunten en stappenplan integraal privacybeleid

Stappenplan privacybescherming voor het sociaal domein

Inhoud

1.Inleiding

Privacybeleid is praktischer dan vaak wordt gedacht en begint aan de top. De Wet Bescherming Persoonsgegevens (WBP) stelt het college van B&W tot taak om te waarborgen dat de personen over wie de gemeente gegevens bijhoudt (of laat bijhouden), op een passende manier beschermd worden tegen de risico's van de informatiemaatschappij. In artikel 6 WBP wordt het college daarom opgedragen om ervoor te zorgen dat persoonsgegevens steeds in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt. Er is een directe relatie met de beginselen van behoorlijk bestuur.[1] Het voorgaande beperkt zich niet alleen tot de eigen bedrijfsvoering maar speelt ook door in samenwerking met anderen.

Zoals hierna zal blijken, vraagt privacy om een heldere bestuurlijke visie op privacy en duidelijke beleidskaders. De 'privacy management key controls' in hoofdstuk 3 laten zien dat privacybeleidsvoering weinig lijkt op het beeld dat de meeste mensen hebben van privacy. In essentie leest de WBP als een managementhandboek voor duurzame vormgeving van de administratieve organisatie. De wet schept ruimte voor gemeentelijke taakuitoefening, efficiëntie en innovatie, maar geeft ook aan waar ethisch en juridisch de grenzen liggen zodat de gemeente gebalanceerd kan omgaan met de belangen van rechten van personen.

Binnen de gemeente is m.b.t. privacy op thematisch gebied al veel geregeld. De huidige decentralisatie vraagt, ook vanuit wetgeving, om een samenhangend integraal beleid, dat als kapstok dient voor de verdere uitwerking binnen de gemeentelijke processen en de samenhang met samenwerkende partijen.

De VISD[2] Privacyscan van KING[3] en VNG wordt momenteel binnen de gemeente uitgevoerd en zal input leveren voor het te volgen stappenplan.

1.1 Positieve privacy impact

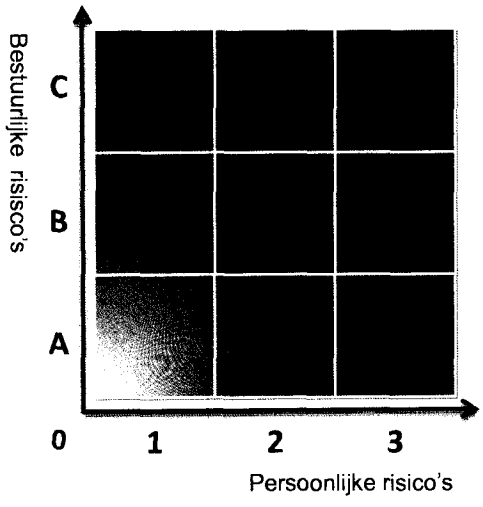
Bij *good privacy governance* verklaart de WBP de gemeentelijke aanpak rechtmatig en respecteert de gemeente de privacy: het doel van de WBP is bereikt.[4] Gegevensverwerking vindt plaats op een faire, veilige en betrouwbare manier waardoor zorg- en hulpbehoevenden op maat geholpen worden. De positieve gevolgen voor de persoonlijk levenssfeer (privacy impact) bestaat bijvoorbeeld uit de stopzetting van huiselijk geweld of het realiseren van optimale thuiszorg.

Een en ander wil niet zeggen dat zich geen enkele fout of discussie meer kan voordoen (perfecte oplossingen bestaan niet) maar de mechanismes om fouten zo goed mogelijk te voorkomen of daar anders snel en adequaat op in te spelen, zijn tot op bestuursniveau ge(waar)borgd. Het college kan met vertrouwen verantwoording afleggen. Privacy kost in principe geen extra inspanningen (werkt in het algemeen juist kostenbesparend) maar is een tweede natuur geworden bij signalering, casusoverleg, gegevensopslag, informatiedeling of bijvoorbeeld de besluitvorming over een persoonlijke voorziening door het college.

[1] TK 26892, nr. 3, p. 14.
[2] VNG Informatievoorziening Sociaal Domein
[3] Kwaliteitsinstituut van de Gemeenten
[4] Art. 6 WBP, art. 10 Grondwet

1.2 Negatieve privacy impact

Bij gebrekkig privacybeleid ontbreken de waarborgen teveel. De gemeente schendt de privacy doordat faire, veilige en betrouwbare gegevensverwerking onvoldoende wordt gegarandeerd. Oplossingen zijn vaak ontoereikend en staan op losse schroeven omdat bijvoorbeeld de aandacht inzakt bij personeelswisselingen.



Privacy Impact Assessment *- Omdat in het sociaal domein vaak wordt gewerkt met bijzondere persoonsgegevens zijn de bestuurlijke en persoonlijke risico's al snel hoog (PIA-score C3).*

Bij gebrekkig privacybeleid is het college aansprakelijk bij incidenten[5] en onnodig kwetsbaar voor discussie. Er kunnen met succes rechtszaken worden aangespannen. Daarnaast kan de landelijke toezichthouder, het College Bescherming Persoonsgegevens (CBP) ingrijpen en vanaf 2015 ook hoge bestuurlijke boetes opleggen (zie p. 7). De reputatieschade en herstelkosten kunnen bijzonder fors blijken en leiden tot ernstig maatschappelijk vertrouwensverlies. De zorg- en hulpverlening kan daardoor ernstig bemoeilijkt worden.[6]

De risico's van gebrekkig privacybeleid voor personen kunnen variëren van ongemak, substantiële benadeling of hinder tot ernstige sociale beschadiging of gevaren voor de gezondheid en de persoonlijke veiligheid. Omdat bij gegevensverwerking in het sociaal domein vaak wordt gewerkt met hoge impact-informatie zoals medische gegevens, gegevens over iemands financiële situatie of strafrechtelijke gegevens, moet worden uitgegaan van hoge privacyrisico's. Het verdient de aanbeveling om goed gebruik te maken van de lessen uit het onderzoeksrapport van de Inspectie Veiligheid en Justitie naar gebrekkige sturing op gegevenskwaliteit in de vreemdelingenketen. De processen in die keten hebben dermate hoge privacy impact dat een verkeerd signaal concreet leidde tot zelfmoord ('er stond een vinkje verkeerd').[7]

1.3 Doel van deze notitie

Deze notitie bevat een stappenplan voor de verdere optimalisering van het privacybeleid van de gemeente tot het wettelijk niveau. Hoofdstuk 2 begint met een korte toelichting op privacy voor scherper zicht op het thema. In hoofdstuk 3 komen de privacy management controls aan bod. In hoofdstuk 5 volgen de te nemen stappen.

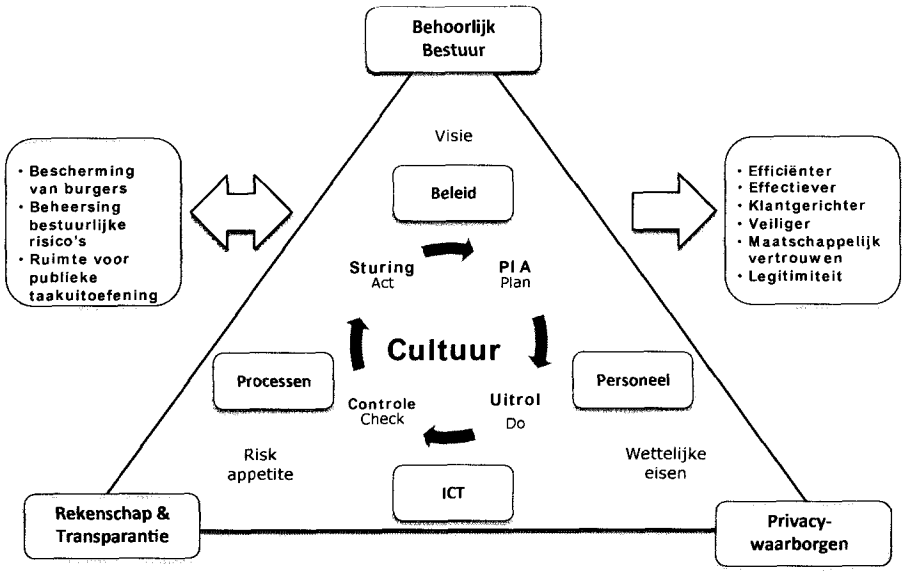
Het college wordt geadviseerd de aanbeveling om de beleidsuitgangspunten op privacy in deze notitie over te nemen en te bevorderen dat het stappenplan ook daadwerkelijk wordt uitgevoerd. Op deze manier voorziet de gemeente niet alleen in het juiste privacybeleid voor het sociaal domein maar speelt het college ook goed in op de aanscherping van privacywetgeving - met name de invoering van de Algemene Verordening Gegevensbescherming van de Europese Unie na 2015.

- ✓ Goedkeuring van deze notitie bewijst direct good governance en biedt een eerste bescherming tegen bestuursaansprakelijkheid terwijl dit leidt tot betere bescherming van privacy door de gemeente.
- ✓ Dat bewijs van good governance wint aan kracht wanneer het college tevens een privacyfunctionaris aanwijst (zie pagina 9). Het college verwerft daarmee krediet bij het College

[5] Art. 49 WBP.
[6] Vgl. fd.nl/ondernemen/902603/ing-schuift-commercieel-uitbaten-klantgedrag-op-lange-baan
[7] https://www.ivenj.nl/actueel/inspectierapporten/rapport-het-overlijden-van-alexander-dolmatov.aspx?cp=131&cs=64448. Vgl. www.rekenkamer.nl/Publicaties/Onderzoeksrapporten/Introducties/2014/10/Basisregistraties

Bescherming Persoonsgegevens terwijl de privacyfunctionaris als buffer kan fungeren in de onderlinge relatie.[8]

✓ De belangrijkste stap die daarna volgt is om zo snel mogelijk algemeen gemeentelijk privacybeleid vast te stellen (hierna: overkoepelend privacybeleid).



Integrale privacybeleidsvoering – privacy wordt organisatiebreed gemanaged op basis van de waarborgen / controls en de bijbehorende beleidsdocumentatie.

[8] Zoals het CBP ook zelf heeft uitgesproken bij het Nederlands genootschap van privacyfunctionarissen NGFG.

2.Toelichting op privacy

Wanneer over privacy wordt gesproken, is het voor goede begripsvorming van belang om drie vormen van privacy te onderscheiden:

- huiselijke privacy;
- lichamelijke privacy;
- gegevensprivacy.

In het sociaal domein spelen deze vormen van privacy in veel gevallen alle drie een rol omdat woningen moeten worden betreden, lichamelijke, psychische of medische zorg vaak de kern van de zaak is, terwijl zorg- of hulpverlening afhankelijk zijn van gegevensverwerkingen zoals verslagen, dossiers, casusoverleg, besluitvorming door het college en voortgangsmonitoring en verrekeningen.

2.1 Privacybescherming: wel of geen toestemming

Het onderscheid tussen de drie vormen van privacy is belangrijk omdat 'het recht op privacy' per vorm een andere betekenis krijgt en ook juridisch en praktisch andere consequenties heeft. Dat geldt met name voor de *bescherming* van het recht op privacy.

- Bij huiselijke en lichamelijke privacy ligt de privacybescherming besloten in de toestemming die gevraagd moet worden voordat mag worden overgegaan tot zorg- of hulpverlening (opt-in). De Wet Maatschappelijke Ondersteuning 2015 en de Jeugdwet geven expliciet aan in welke gevallen zorg- of hulpverlening met - of juist zonder toestemming kan plaatshebben.

- Bij gegevensprivacy is het precies andersom. De privacybescherming ligt juist *niet* besloten in toestemming en hoeft alleen bij uitzondering worden gevraagd.[9] Het is in strijd met de wet om toestemming te vragen in de situaties waarin dat wettelijk buiten de orde is.[10] Dit betreft onder andere de verwerking van 'bijzondere persoonsgegevens', zoals medische gegevens, gegevens over iemands herkomst of geloofsovertuiging.

Wie instemt met zorg- of hulpverlening, kan of moet begrijpen dat hiervoor verwerking van gegevens noodzakelijk is. Het is aan de gemeente om, begrijpelijk uit te leggen welke privacybeschermende maatregelen zijn genomen om onrechtmatig gebruik van deze gegevens te voorkomen.. Hierbij hoort ook informatie over de manier waarop iemand zijn privacyrechten kan uitoefenen, zoals de rechten op inzage en correctie of het zojuist genoemde recht van bezwaar (recht van verzet als bedoeld in art. 40 WBP).

2.2 Grondslagen

De wet erkent verschillende situaties waarin gegevensverwerking als vanzelfsprekend ('noodzakelijk') moet worden beschouwd:[11]

1. gegevens zijn nodig voor de totstandkoming of uitvoering van een overeenkomst – denk aan een behandelingsovereenkomst;
2. de gegevensverwerking is wettelijk verplicht – bijvoorbeeld verplicht gebruik van de verwijsindex risicojongeren;

---

[9] Bijvoorbeeld bij deling door jeugdhulpverleners van hun dossiergegevens met derden (artikel 7.3.11 Jeugdwet) of wanneer de gemeente gegevens wil afnemen van zorgverzekeraars of zorgaanbieders (artikel 5.1.1 lid 5 WMO).

[10] Zie ook TK 25892, nr 3, p. 9 en 80. Dit is onder meer ook het punt dat het CBP maakt in de brief van 30 oktober 2014 (zie: www.cbpweb.nl/downloads_pb/pb_20141111_advies-privacytoets-jeugdhulpdomein.pdf).

[11] Art. 8b t/m 8f WBP

3. de gegevens zijn nodig voor bescherming van vitale belangen – bijvoorbeeld signalering van kindermishandeling;
4. de gegevens zijn nodig voor de goede vervulling van publieke taken – bijvoorbeeld de feiten die bekend moeten zijn voor zorgvuldige besluitvorming over passende voorzieningen;
5. de gegevensverwerking is nodig voor andere gerechtvaardigde belangen – bijvoorbeeld het opsporen van fraude of misbruik van gemeentelijke voorzieningen.[12]

2.3 Schending van de gegevensprivacy

Het voorgaande wil niet zeggen dat de gemeente de vrije teugel heeft om gegevens te verzamelen of deze breed toegankelijk te maken. Zonder praktische maatregelen op het gebied van gegevensdosering (proportionele informatievoorzieningen) en de juiste 'waterscheidingen' om te voorkomen dat gegevens te gemakkelijk voor andere doelen kunnen worden gebruikt (doelbinding), vervalt alsnog de legitimiteit van de gegevensverwerking. Er zijn ook andere manieren waardoor de legitimiteit van de gegevensverwerking vervalt. Zie hiervoor met name de punten A t/m G op pagina 9. De gemeente schendt de gegevensprivacy wanneer er iets schort aan *alle* punten op deze pagina, maar punten A t/m G zijn meest acuut.

2.4 Bestuursaansprakelijkheid

Bij schending van de gegevensprivacy is het college wettelijk aansprakelijk. Iedere benadeelde heeft dan recht op schadevergoeding.[13] De landelijke toezichthouder, het College Bescherming Persoonsgegevens (CBP) – die binnenkort de Autoriteit Gegevensbescherming gaat heten – kan op ieder moment onderzoek instellen en dwangmaatregelen opleggen (last onder dwangsom). Vanaf 2015 is het CBP daarnaast bevoegd tot het geven van bestuurlijke boetes. In eerste instantie gaat het om boetes tot 810.000 Euro. Het Europese Parlement dringt bij de totstandkoming van de nieuwe EU-brede privacywetgeving (Algemene Verordening Gegevensbescherming - AVG) aan op boetes tot 100 miljoen Euro. Naar verwachting wordt de AVG in 2015 goedgekeurd waarna een invoeringstermijn volgt van twee jaar. De huidige Wet Bescherming Persoonsgegevens (WBP) wordt dan ingetrokken.

De kans op bestuursaansprakelijkheid wordt extra groot door twee vernieuwingen:

- de invoering van de plicht om gegevensbeveiligingsincidenten te melden bij het CBP ('meldplicht datalekken'). Dergelijke meldingen zijn voor het CBP een signaal dat er sprake is van gebrekkig privacy management;
- de invoering van een documentatieplicht. Op het niet beschikken over beleidsdocumentatie wordt in de AVG eveneens een boete gesteld. Om vast te stellen of er sprake is van gebrekkig privacy management hoeft het CBP alleen maar die documentatie op te vragen. Het niet kunnen produceren van stukken is daarmee direct al een brevet van onvermogen. Het gelaagde stelsel op p. 9 is in belangrijke mate bedoeld om het college in staat te stellen om op ieder moment verantwoording te kunnen afleggen.

[12] Vgl. art. 2.9d Jeugdwet.

[13] Art. 49 WBP.

3. Uitgangspunten privacybeleid

Voldoen aan wetgeving op de gegevensprivacy betekent dat de gemeente structureel de onderstaande privacywaarborgen biedt.[14] De waarborgen zijn tegelijkertijd ook de handvatten (controls) om op privacy te sturen.

Alle in dit hoofdstuk genoemde aandachtpunten moeten op groen staan wil er sprake zijn van behoorlijke en zorgvuldige gegevensverwerking in overeenstemming met de wet.

3.1 Beleidsmatige privacywaarborgen

1. **Privacy management:** pro-actieve sturing door het college om de gegevensprivacy van burgers en medewerkers te waarborgen, onder meer door duidelijke afbakening van rollen en verantwoordelijkheden.
2. **Beleid:** een goed gedocumenteerd stelsel van interne afspraken om persoonlijke en gemeentelijke belangen te beschermen.
3. **Ketenregie:** een goed gedocumenteerd stelsel van afspraken met ketenpartners en uitvoeringsorganisaties – met name bij samenwerking binnen een gemeenschappelijke regeling.
4. **Beleidstransparantie:** doelgroepgerichte uitleg over het gemeentelijk privacybeleid.
5. **Service:** klantgericht inspelen op vragen over het privacybeleid, klachten en verzoeken om inzage, correctie en – voor zover de wet daartoe verplicht – stopzetting en verwijdering van gegevens.
6. **Toezicht:** controle op de privacybestendigheid van de organisatie, bij voorkeur door een onafhankelijke privacyfunctionaris (zie hierna) en desnoods ondersteund door audits.
7. **Accountability:** het vermogen om op ieder gewenst moment verantwoording te kunnen afleggen over de naleving van privacywetgeving, zoals aangegeven in de vorige paragraaf.

3.2 Operationele privacywaarborgen

A. **Subsidiariteit:** privacybestendigheid weegt zwaar bij de vormgeving van informatievoorzieningen en oplossingen voor gegevensuitwisseling. Voor zover een en ander te rijmen valt met andere kwaliteitseisen en kostenafwegingen, wordt gekozen voor de meest privacybestendige optie.
B. **Legitimiteit:** gegevensverwerking vindt uitsluitend plaats voor zover dit nodig voor goede gemeentelijke taakuitoefening is of om andere redenen wettelijk wordt toegestaan.
C. **Doelbinding:** gegevens worden gebruikt voor duidelijk omschreven doelen en kunnen alleen worden gebruikt voor andere doelen of worden gedeeld met derden voor zover de wet dat toestaat.
D. **Kwaliteit:** gegevens zijn steeds voldoende actueel en zijn een nauwkeurige weergave van de feitelijke situatie.
E. **Proportionaliteit:** de gegevensverwerking is steeds geoptimaliseerd aan de hand van de functionele informatiebehoefte waarbij ook rekening is gehouden met de belangen van betrokkenen.
F. **Informatieveiligheid:** er wordt goed gelet op het bestaan van geheimhoudingsafspraken en gegevens worden passend beveiligd.[15]
G. **Houdbaarheid:** gegevens die niet langer nodig zijn, worden vernietigd of gearchiveerd.

3.3 Afbakening rollen en verantwoordelijkheden

De wet wijst het college aan als de probleemeigenaar van privacybeleidsvoering,[16] maar het college zal op haar beurt verantwoordelijkheden aan anderen moeten opdragen. Ook op lager niveau dienen rollen en verantwoordelijkheden duidelijk te zijn. Er zijn afspraken nodig over het afleggen van

[14] Vgl. kernbepalingen van de WBP en de AVG.
[15] Informatiebeveiliging bij voorkeur op basis van een daarvoor geschikte standaardnormering zoals ISO 27000.
[16] Art. 1d WBP. Zie ook TK 25892, nr. 3, p 57. Voorts art. 1.3 lid 3 Jeugdwet, art. 1.2.1.a WMO en art. 7 Participatiewet

interne verantwoording. Uiteindelijk is iedereen op zijn eigen manier verantwoordelijk voor geslaagde privacybeleidsvoering. Het college blijft in alle gevallen eindverantwoordelijk.

3.4 Gelaagde aanpak en documentatie

Privacybeleid kent een gelaagdheid die het beste ook in de beleidsdocumentatie tot uitdrukking wordt gebracht en waarbij documenten op een logische manier met elkaar samenhangen.

- **Overkoepelend privacybeleid**: er is een kapstok/raamwerk waarin de algemene aspecten van de gemeentelijke privacybeleidsvoering wordt geregeld: missie, wijze van sturing, middelen, toezicht en handhaving.
- **Themabeleid:** generieke aspecten van privacybeleidsvoering voor de gemeentelijke taken (privacybeleid voor het sociaal domein, burgerzaken, openbare orde en veiligheid, personeelszaken) worden ook op generiek niveau beschreven. Themabeleid wordt ook opgesteld aan de hand van thematische privacy impact assessments (PIA's) zoals een 'PIA Sociaal Domein'.
- **Procesplannen**: Het themabeleid wordt nader uitgewerkt voor de afzonderlijke processen binnen de domeinen jeugdzorg, maatschappelijk ondersteuning en participatie. Procesplannen beschrijving de mix van maatregelen waarmee de privacybescherming rondom een bepaald proces op een passende / evenwichtige manier wordt gewaarborgd.
- **Implementatie**, procesplannen krijgen concrete invulling aan de hand van bijvoorbeeld concrete afspraken over de informatiebeveiliging van een proces, de formulering van een protocol of doelgroepgerichte training en voorlichting.

4 De privacyfunctionaris

De WBP adviseert het college om zich te laten bijstaan door een privacyfunctionaris, wat na 2015 mogelijk ook verplicht wordt. 'Functionaris' is eigenlijk niet het goede woord. In de Engelstalige beleidsstukken van de EU wordt gesproken van een 'data protection *officer*'. Hij is als het ware de privacy-accountant van de gemeente en is tevens de ombudsman voor burgers bij klachten over de serviceverlening van de gemeente bij de uitoefening van privacyrechten en de privacybeleidsvoering. Als toezichthouder heeft hij een belangrijke beleidscoördinerende rol. Hij adviseert over oplossingen en kan daarover een wettelijk zwaarwegend oordeel afgeven, waar ook het CBP niet omheen kan. Iemand is geschikt als privacyfunctionaris als over de volgende kwaliteiten beschikt:[17]

- expert op het gebied van privacywetgeving;
- praktijkdeskundig (kennis van organisaties, processen, ICT en informatiebeveiliging);
- onafhankelijk en betrouwbaar;
- gevoel voor de interne en externe verhoudingen;
- beroepservaring die past bij zijn verantwoordelijkheden;
- vaardigheden op het gebied van communicatie, PR en regulatory affairs.

Een privacyfunctionaris kan intern worden aangesteld, worden ingehuurd of worden betrokken via een organisatie waarbij de gemeente is aangesloten. Hij behoort te worden aangemeld bij het CBP,[18] die zijn gegevens overneemt in het openbare register van privacyfunctionarissen.[19] Het CBP beoordeelt niet de geschiktheid van de privacyfunctionaris.

[17] Art. 63 WBP en vergelijkbare vereisten in de AVG

[18] www.cbpweb.nl/downloads_melden/fg_aanmeldingsformulier.pdf

[19] www.cbpweb.nl/Pages/ind_reg_fgreg.aspx

5 Stappenplan

Stap 1 – Goedkeuring van deze notitie

- Beleidsvisie op privacy
- Bestuurlijke commitment
- Aantoonbaar begin van good governance (bewijs)

Stap 2 – Aanwijzing privacyfunctionaris

- Inrichting privacy office (taken, plaats in organisatie, rapportagelijnen, middelen)
- Keuze voor een geschikte persoon
- Melding bij het CBP

Stap 3 – Realisering van overkoepelend privacybeleid

- Formulering en goedkeuring bestuurlijk privacybeleid
- Formulering communicatiestrategie op hoofdlijnen
- Inrichting incident managementprocedure
- Inrichting verantwoordingsprocedures
- Inrichting privacyservices
- Informeren gemeenteraad
- Update privacy statement website

Stap 4 – Realisering specifiek privacybeleid

- Stand van zaken-analyse en prioritering
- Uitvoering van privacy impact assessments op gemeentelijke processen
- Inventarisatie van bijzondere wettelijke verplichtingen volgens materiewetten
- Vertaling naar themabeleid en procesplannen
- Eventueel check bij CBP
- Besluitvorming op themabeleid en procesplannen
- Terugkoppeling aan de raad en voorlichting aan inwoners

Stap 5 – Uitwerking en implementatie

- Conform de actiepunten uit de procesplannen
- Aandacht voor convenanten, protocollen, inkoopcontracten en andere samenwerkingsafspraken.
- Voorlichting en trainingen
- Aandacht voor individuele geheimhoudingsafspraken, gedragsafspraken
- Aandacht voor juridische formaliteiten zoals meldingen van gegevensverwerkingen bij het CBP

Stap 6 – Beheer en evaluatie

- Controle op naleving afspraken via 'in control-statements' en/of audits
- Advies over de stand van zaken en verbeterpunten door de privacyfunctionaris
- Evaluatie & optimalisering gemeentelijk privacybeleid waar nodig
- Terugkoppeling stand van zaken en bijsturingsbesluiten aan de raad
- Publieksinformatie over de privacybeleidsvoering
- Optioneel: informeren CBP