gemeente Hoeksche Waard

GEMEENTEBLAD

Officiële uitgave van de gemeente Hoeksche Waard

Nr. 74704

29 maart

2019

Besluit van het college van burgemeester en wethouders van de gemeente Hoeksche Waard houdende regels omtrent Privacybeleid gemeente Hoeksche Waard

1. Inleiding

1.1 Privacy: persoonlijke levenssfeer

Gemeente Hoeksche Waard verwerkt persoonsgegevens van onder andere haar inwoners. De verwerking van deze gegevens is aan wet- en regelgeving gebonden en inwoners moeten er op kunnen vertrouwen dat hun gegevens bij de gemeente in goede handen zijn. In dit beleid worden de kaders waarbinnen de gemeente persoonsgegevens opvraagt, opslaat, bewerkt, bewaart, deelt en vernietigt beschreven. Bescherming en een zorgvuldige en behoorlijke verwerking van persoonsgegevens staan centraal.

'Privacy' is een ruim begrip: het gaat om de bescherming van persoonsgegevens, de bescherming van de persoonlijke levenssfeer (lichaam, familie- en gezinsleven, woning e.d.) en het recht op vertrouwelijk communiceren. Persoonlijke gegevens en communicatie hebben in deze tijd te maken met geautomatiseerde systemen. Deze systemen moeten technisch en voor het gebruik beveiligd zijn waardoor de informatie van personen 'in' deze systemen voldoet aan de eisen van de privacywetgeving. Door deze vervlechting van persoonsgegevens en informatie via geautomatiseerde systemen zijn privacy en informatiebeveiliging onlosmakelijk met elkaar verbonden.
Door de verbondenheid van persoonsgegevens en geautomatiseerde systemen kan het Privacybeleid niet los gezien worden van het Strategisch Informatiebeveiligingsbeleid en het Jaarplan Informatiebeveiliging (deze documenten zijn terug te vinden op Samen@Work).

Persoonsgegevens zijn gegevens die herleidbaar zijn naar een (natuurlijk) persoon.
Formeler gezegd: het gaat om alle gegevens over een geïdentificeerde of identificeerbaar persoon. Dit kan bijvoorbeeld iemands naam zijn, adresgegevens of een e-mailadres, maar ook meer indirecte gegevens kunnen persoonsgegevens zijn, zoals een bankrekeningnummer. Doorslaggevend is dat de gegevens over een persoon gaan van wie de identiteit door de gemeente - of door een ander - zonder onevenredige inspanning kan worden vastgesteld.

1.2 Privacy in de context

Op het gebied van privacy zijn er diverse ontwikkelingen in Europees en nationaal verband. Vanaf mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing, de Europese verordening die in alle lidstaten directe werking heeft en daarmee wet is geworden. Sinds 1 januari 2016 geldt in Nederland de meldplicht datalekken.
Regelmatig verschijnen er in de media artikelen over privacy en burgers stellen vaker vragen over de bescherming van hun persoonlijke levenssfeer. De risico's van onvoldoende bescherming van privacy worden ook steeds groter en duidelijker.

1.2.1 Privacy bij gemeente Hoeksche Waard

De 5 gemeenten in de Hoeksche Waard en de gemeenschappelijke regelingen hebben de afgelopen jaren op dit vakgebied niet stilgezeten. Vooral in het Sociaal Domein en bij Burgerzaken is de afgelopen jaren al gewerkt aan de bescherming van persoonsgegevens. Ook is een begin gemaakt met het implementeren van de maatregelen vanuit de Baseline Informatiebeveiliging Gemeenten (BIG). Na de diverse acties die vanaf 2016 zijn ingezet is nu de fase aangebroken om de bescherming van persoonsgegevens in samenhang met informatiebeveiliging tot uitvoering te brengen voor gemeente Hoeksche Waard, waarbij de verschillende activiteiten en maatregelen op elkaar worden afgestemd en in samenhang worden uitgevoerd.
De activiteiten en maatregelen die de komende tijd worden uitgevoerd zijn SMART opgenomen in het Jaarplan Privacy en het Jaarplan Informatiebeveiliging.

1.3 Over dit beleid

1.3.1 Wet- en regelgeving

De verwerking van persoonsgegevens is gebonden aan eisen uit wet- en regelgeving. Naast de Algemene Verordening Gegevensbescherming (AVG), kunnen dit ook specifieke wetten zijn, zoals de Wet maatschappelijke ondersteuning (Wmo 2015), de Jeugdwet of de Wet basisregistratie personen. Gemeente Hoeksche Waard stelt met dit Privacybeleid de kaders en formuleert uitgangspunten over het zorgvuldig omgaan met persoonsgegevens binnen de kaders van de verschillende wetten. Het Privacybeleid wordt door het college van B&W vastgesteld en is bedoeld voor de gemeentelijke organisatie en voor de ketenpartners waarmee samengewerkt wordt.

De kaders uit dit beleid vormen het uitgangspunt voor nader uit te werken gedragsrichtlijnen, reglementen, procedures en/of protocollen (of om deze te actualiseren). Deze richtlijnen ed. geven richting aan de uitvoering in de dagelijkse praktijk. Het gaat in ieder geval om (niet limitatief):

- Privacyreglement, dat concreter is dan het beleid en nader ingaat op diverse onderwerpen zoals rechten van betrokkenen, bijhouden van een register van verwerkingen en de wijze waarop de gemeente omgaat met datalekken;
- Privacyprotocol, dat richtlijnen en handvatten voor alle medewerkers bevat;
- Reglement gebruik e-mail, internet en social media en overige ICT-middelen voor alle medewerkers;
- AI dan niet verplichte procedures per werkproces waarin frequent en systematisch persoonsgegevens worden verwerkt;
- Procedure datalekken.

Naast deze kunnen in de toekomst nog meer richtlijnen ed. passend binnen de kaders van het beleid worden opgesteld. Hiermee kan de gemeente snel en flexibel inspelen op nieuwe ontwikkelingen.

De onderlinge samenhang tussen diverse documenten is vastgelegd in de Privacymatrix gemeente Hoeksche Waard (als bijlage bijgevoegd).

1.3.2 Samenhang Privacybeleid met Informatiebeveiligingsbeleid

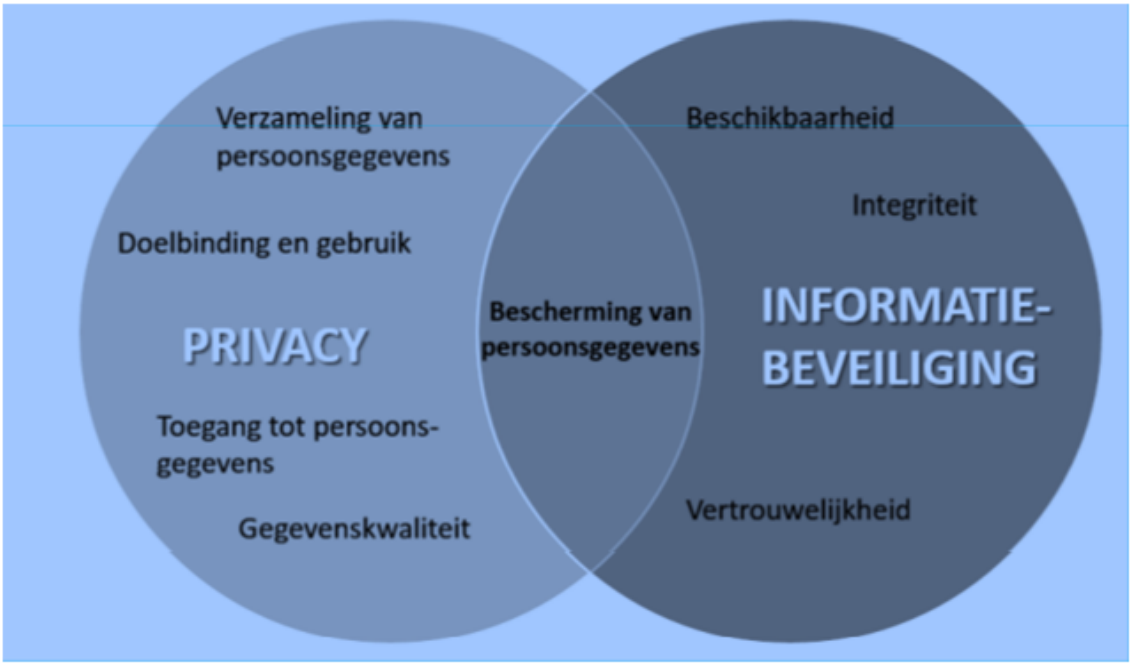
Zoals al in de inleiding beschreven is er nauwe samenhang tussen de bescherming van persoonsgegevens en informatiebeveiliging. Informatiebeveiliging gaat ook over vertrouwen in de bescherming van informatie in de persoonlijke levenssfeer (privacy) zoals vastgelegd in dit Privacybeleid.

In het Strategisch Informatiebeveiligingsbeleid worden de strategische uitgangspunten en verantwoordelijkheden ten aanzien van de gemeente op het gebied van informatiebeveiliging en gegevensbescherming benoemd, welke als basis dienen voor de Tactische Richtlijnen Informatiebeveiliging. De betrouwbaarheid (beschikbaarheid, integriteit) van informatiesystemen en vertrouwen in informatie (privacy, controleerbaarheid) zijn dan ook van groot belang. Ook burgers, bedrijven en ketenpartners verwachten betrouwbare informatie.

<u>Rollen</u>

De Functionaris Gegevensbescherming (FG) heeft onder meer als taken het toezien op naleving van privacywetgeving en adviseren over het beschermen en borgen van een juiste verwerking van persoonsgegevens in werkprocessen conform de wetgeving.
De Privacy Officer (PO) voert onder aansturing van de directie taken uit op het gebied van de privacybescherming die voortvloeien uit het Privacy beleid.
De Chief Information Security Officer (CISO) bevordert en adviseert gevraagd en ongevraagd over Informatiebeveiliging aan de directie en rapporteert volgens de gebruikelijke P&C-cyclus concern breed aan de directie over de risico's, veranderingen in controlemaatregelen en planning.

Samenhang Privacy en Informatiebeveiliging:



2. Visie, strategische uitgangspunten en kaders

2.1 Visie

'De inwoners van gemeente Hoeksche Waard en partijen die samenwerken met de gemeente kunnen erop vertrouwen dat de gemeente hun privacy respecteert en zorgvuldig omgaat met hun persoonsgegevens. De bescherming van persoonsgegevens past de gemeente toe in de dienstverlening en in de beleidskeuzes die gemaakt worden conform het Privacybeleid. Technologische en maatschappelijke ontwikkelingen dwingen de gemeente ertoe het Privacybeleid voortdurend aan te passen. In de afwegingen zijn wetgeving en de 'menselijke maat' voor het beschermen van de privacy van de inwoners en samenwerkende partijen belangrijke kaders. Privacybescherming is een onderwerp dat voor bestuurders en medewerkers een integraal onderdeel van het werk vormt.'

2.2 Strategische uitgangspunten

De gemeente hanteert de volgende uitgangspunten bij het uitwerken van richtlijnen, protocollen, procedures of reglementen en de inrichting van de organisatie:

Zorgvuldig en werkbaar

Gemeente Hoeksche Waard verwerkt voor de uitvoering van haar publieke taken persoonsgegevens. Deze gegevens worden, meestal door inwoners, veelal vrijwillig, maar soms ook verplicht afgestaan. Soms gaat het ook om vertrouwelijke gegevens. De beschikbaarheid, integriteit en vertrouwelijkheid van deze gegevens moet worden gewaarborgd (informatiebeveiliging). Inwoners moeten erop kunnen vertrouwen dat de gemeente zorgvuldig met persoonsgegevens omgaat, en dat de gemeente voorkomt dat er een onnodige of te vergaande inbreuk wordt gemaakt op de persoonlijke levenssfeer.
Het waarborgen van de persoonlijke levenssfeer binnen de kaders van de wet- en regelgeving, moet niet in de weg staan aan een goede en tijdige uitvoering van de gemeentelijke taken, bijvoorbeeld bij zorgverlening of openbare orde en veiligheid. Het beleid voor de verwerking van persoonsgegevens moet met andere woorden niet dusdanig ingewikkeld of rigide zijn, dat het in de weg staat aan de zorg- en dienstverlening. Bescherming van persoonsgegevens en rechten die burgers kunnen doen gelden ten aanzien van die verwerking zijn geen absolute rechten. Deze moeten afgewogen worden ten opzichte van andere belangen, bijvoorbeeld veiligheid. Soms kan er een situatie ontstaan dat wetgeving onderling strijdig lijkt te zijn. Mocht deze situatie zich voordoen, dan gaat de gemeente Hoeksche Waard daar weloverwogen en zorgvuldig mee om. Waar nodig en mogelijk wordt het advies en de deskundigheid van wetgever, toezichthouder of koepelorganisatie betrokken bij dilemma's.
Transparant en open

Het is van belang dat inwoners vertrouwen hebben in de zorgvuldige verwerking van hun persoonsgegevens. Inwoners krijgen inzicht in en worden helder geïnformeerd over hun rechten, en de wijze waarop hun persoonsgegevens worden verwerkt en beheerd. Voor hen moet duidelijk zijn:

- Welke persoonsgegevens de gemeente verzamelt (wat) en
- met welk doel (waarom),
- wie toegang heeft tot deze gegevens (wie) en
- wat de gemeente vervolgens verder doet met deze gegevens (wat gebeurt er),
- hoe lang de gegevens bewaard worden (bewaartermijnen) en
- hoe de gegevens beveiligd worden.

Gemeente Hoeksche Waard geeft gehoor aan verzoeken van betrokkene die rechten conform de AVG wil uitoefenen, zoals bij een verzoek om inzage en/of correctie. Voor deze verzoeken wordt een procedure opgesteld en werkprocessen ingericht om deze gestructureerd te kunnen behandelen.

Iedere betrokkene heeft het recht op informatie over de persoonsgegevens die de gemeente van hem of haar verwerkt en over het doel waarmee de gegevens worden verwerkt, om deze in te zien en ook om deze gegevens te verbeteren, aan te vullen te verwijderen of af te schermen als deze feitelijk onjuist, onvolledig of niet ter zake dienend zijn. Het college van B&W communiceert actief over deze rechten, op de gemeentelijke website en in andere uitingen. Het college van B&W draagt zorg voor een eenvoudige en toegankelijke wijze waarop burgers hun rechten kunnen uitoefenen.
Transparantie zal niet in alle gevallen opgaan. Er kan sprake zijn van legitieme uitzonderingen, bijvoorbeeld in situaties die te maken hebben met openbare orde en veiligheid. In dergelijke gevallen zal de gemeente, met inachtneming van wet- en regelgeving, een voorbehoud kunnen maken op het transparantiebeginsel.
Bij transparantie hoort ook een open cultuur. De open cultuur helpt de gemeente bij het verder op orde krijgen van het Privacybeleid en -beheer. Wij moedigen medewerkers aan incidenten te melden, hiervoor is een laagdrempelige procedure ingericht (in Topdesk). Ook inwoners kunnen situaties makkelijk en snel melden, via de reguliere klachtenprocedure en waar nodig ook via een aparte klachten- en meldingsprocedure. De gemeente legt verantwoording af over de uitvoering van het Privacybeleid, inclusief de opgetreden incidenten en klachten.

Privacy by design en dataminimalisatie

Bij de inrichting van een werkproces - inclusief de bijbehorende ICT-infrastructuur - is het van groot belang om direct te bedenken welke vragen en problemen vanuit privacy-oogpunt in en rondom dat werkproces een rol (kunnen) spelen. Gebeurt dat, en worden daarbij goede oplossingen bedacht en ingeregeld, dan wordt er aan de voorkant voor gezorgd dat bepaalde privacy problemen zich niet kúnnen voordoen.
Denk bijvoorbeeld aan een logische en strakke toegangsbeveiliging, encryptie van gegevens, het scheiden van databestanden, of het automatisch verwijderen van gegevens na een bepaalde periode of gebeurtenis. Dit noemen we 'privacy by design'. Privacy by design is van grote betekenis om in control te komen en te blijven op privacygebied en de informatiebeveiliging.
Zorgvuldig met privacy omgaan, betekent ook dat de gemeente niet onnodig of te veel persoonsgegevens opvraagt, deelt of bewaart. Het uitgangspunt is dan ‘dataminimalisatie’. Dit betekent dat de gemeente alleen die gegevens verwerkt die noodzakelijk zijn voor de uitoefening van haar taak. Dit uitgangspunt wordt bij de inrichting van werkprocessen en informatiesystemen gehanteerd.

Reikwijdte

Dit Privacybeleid is van toepassing op het bestuur en de medewerkers van de gemeente Hoeksche Waard, inclusief alle extern ingehuurde medewerkers. De reikwijdte van het beleid strekt zich voor zover van toepassing ook uit tot externe verwerkers van gegevens waarvoor de gemeente volgens de AVG verantwoordelijk is. Bij de uitbesteding van taken aan private partijen, zoals ICT-leveranciers en zorgverleners, blijft het college van B&W verantwoordelijk voor de goede uitvoering van die taken en voor de naleving van de AVG. Dat betekent dat wanneer sprake is van het verwerken van persoonsgegevens door een externe verwerker voorafgaand aan de verwerking daarvan schriftelijke afspraken worden gemaakt, waarbij er een vertaalslag wordt gemaakt van het Privacybeleid en er rekening wordt gehouden met de eisen die de AVG stelt. Deze afspraken worden vastgelegd in contracten met derden (verwerkersovereenkomsten bij inkoopcontracten) of in convenanten/protocollen met samenwerkingspartners.

Indien sprake is van structurele uitwisseling of samenwerking met een externe organisatie of met andere gemeente(n), worden schriftelijke afspraken gemaakt over het uitwisselen van persoonsgegevens, de manier waarop dat gebeurt (beveiliging) en over het uitwisselen van andere vertrouwelijke informatie.

2.3 Kaders en wetgeving

Wettelijke kaders

De belangrijkste wettelijke kaders met betrekking tot privacybescherming zijn:
1. Artikel 8 Europees Verdrag voor de Rechten van de Mens
2. Artikel 10 t/m 13 Nederlandse Grondwet
3. Algemene Verordening Gegevensbescherming (AVG)
4. art. 272 Wetboek van Strafrecht
5. Wet maatschappelijke ondersteuning 2015 (Wmo)
6. Jeugdwet
7. Participatiewet
8. Archiefwet

Interne kaders

- Integriteitsbeleid
- Strategisch Informatiebeveiligingsbeleid 2019-2020

3. Organisatie

3.1 Verantwoording aan de Raad

Het college legt jaarlijks verantwoording af aan de gemeenteraad over de realisatie en de toepassing van het Privacybeleid via de paragraaf bedrijfsvoering in de jaarstukken.

In de verantwoording in de jaarstukken van de komende jaren, komen de volgende onderwerpen aan de orde:
- Realisatie en uitvoering van het Privacybeleid en integratie van de wettelijke eisen van de AVG in de werkprocessen;
- Per afdeling de inventarisatie en implementatie van: de risico-inventarisatie, classificatie naar vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en het register van verwerkingen van persoonsgegevens conform artikel 30 AVG;
- Bewustwording en training: activiteiten die hebben plaatsgevonden op het gebied van bewustwording en training;
- Rapportage over de aard, omvang en afhandeling van eventuele klachten en meldingen van (vermoedelijke) datalekken;
- Beheer en opslag van persoonsgegevens, de rapportage sluit aan op (rapportages met betrekking tot) het informatiebeveiligingsbeleid en de jaarplannen die daaruit volgen.

Naast de jaarlijkse verantwoording, meldt het college van B&W bijzonderheden ten aanzien van gegevensverwerking en privacy separaat en proactief aan de gemeenteraad in het kader van de actieve informatieplicht. Daaronder valt in ieder geval:
- Ontwikkelingen die zich voordoen op het gebied van privacy en de bescherming van persoonsgegevens. Het college van B&W zal (plannen voor) een dergelijke ontwikkeling voorleggen aan de raad, zodat de raad zich hierover kan uitspreken.
- In geval van een incident met grote impact met persoonsgegevens van bewoners of medewerkers.

3.2 Inrichting en beschrijving van rollen met betrekking tot privacy

3.2 a Gemeenteraad
De gemeenteraad stelt de gemeente brede kaders voor privacy en gegevensverwerking vast, inclusief de daarbij horende middelen. De gemeenteraad controleert het college van B&W bij de uitvoering van deze kaders en wordt hiertoe in staat gesteld door de verantwoordingsinformatie die het college van B&W verschaft.

3.2 b College van B&W
Het college van B&W is integraal verantwoordelijk voor zorgvuldigheid van verwerking van (persoons-) gegevens. Het college van B&W stelt hier voor dit Privacybeleid en het Privacyreglement vast ter

invulling van de kaders en doet de gemeenteraad voorstellen over in te zetten middelen (budget). Het college van B&W legt periodiek verantwoording af aan de gemeenteraad over het gevoerde Privacybeleid.
3.2 c Directie en teammanagers
De directie stelt specifieke gedragsrichtlijnen, reglementen, procedures en/of protocollen met betrekking tot zorgvuldigheid van verwerking van (persoons-)gegevens vast. Directie en teammanagers zijn gezamenlijk verantwoordelijk voor het inrichten van de privacyorganisatie. Zij zijn naar de organisatie en medewerkers kaderstellend en sturend en monitoren de uitvoering van het Privacybeleid. Uitvoerende taken van de directie die voortvloeien uit dit beleid worden gemandateerd aan de teammanagers. De directie en teammanagers stimuleren gezamenlijk kennisvergaring en bewustwording bij medewerkers. De teammanagers zijn ook verantwoordelijk voor het intern melden van datalekken bij de juiste behandelaars en via de juiste weg en voor de communicatie naar het college van B&W, inwoners en betrokkenen.

3.2 d Functionaris Gegevensbescherming (FG)
Gemeente Hoeksche Waard heeft conform de AVG een Functionaris Gegevensbescherming (FG) benoemd. De FG kan op basis van artikel 37 AVG wat betreft de uitoefening van zijn functie geen aanwijzingen ontvangen van de verantwoordelijke of van de organisatie die hem heeft benoemd. De FG is tevens contactpersoon voor de Autoriteit Persoonsgegevens (AP) en houdt intern toezicht op de naleving van wetgeving en op de opvolging van aanbevelingen uit Privacy Impact Analyses. De FG ondersteunt de organisatie bij het uitvoeren van de meldplicht datalekken en doet de daadwerkelijke melding bij de AP. De FG legt verder periodiek verantwoording af aan de directie. Indien nodig kan verantwoording worden afgelegd aan het college van B&W of de gemeenteraad.
In verband met de onafhankelijke positie zijn de taken en bevoegdheden van de FG in de organisatieregeling vastgelegd.

3.2 e Chief Information Security Officer (CISO)
De CISO houdt toezicht op de informatiebeveiliging en rapporteert hierover aan de directie. Hij bewaakt de voortgang van aanbevelingen uit audits en andere onderzoeken en adviseert over het te voeren beleid.

3.2 f Privacy Officer (PO)
De PO ondersteunt en adviseert directie en teammanagers bij privacyvraagstukken, het opstellen van richtlijnen, protocollen, procedures of reglementen, het afsluiten van verwerkersovereenkomsten, het inrichten van werkprocessen en het actueel houden van het register van verwerkingen.

3.3 Interne samenwerking

Privacy en informatiebeveiliging vereisen een integrale aanpak binnen de gemeente. Daarom vindt intern periodiek overleg plaats tussen CISO, FG, PO, directie en teammanagers en wanneer aan de orde met vakgerichte beveiligingsfunctionarissen.

4. Implementatie en borging

Op het moment van voorleggen van dit Privacybeleid aan het college van B&W voldoet gemeente Hoeksche Waard nog niet aan alle vereisten die de AVG stelt. Dat geldt voor het inzichtelijk hebben en kunnen maken van alle gegevensverwerkingen (het transparantiebeginsel) en het inrichten van de organisatie.

In het Jaarplan Privacy en het Jaarplan Informatiebeveiliging worden de activiteiten beschreven die de komende jaren worden uitgevoerd en maatregelen die worden genomen om te zorgen dat gemeente Hoeksche Waard veilig en zorgvuldig werkt met persoonsgegevens (volledig conform de eigen kaders en de wet- en regelgeving).

De borging van het veilig en zorgvuldig werken met persoonsgegevens conform dit beleid zal plaatsvinden door een adequate inrichting van applicaties, systemen en processen en door middel van bewustwordingscampagnes voor de medewerkers om te zorgen voor voldoende kennis en kunde en de juiste attitude om dit te bewerkstelligen.

Bijlage

PRIVACY MATRIX GEMEENTE HOEKSCHE WAARD									
		INTERN		EXTERN					
DOCUMENTEN		A - Externe medewerker	B - Medewerker	C - Burger	D - Samenwerkende Instantie (SI)	E - Medewerker bij SI	F - Verwerker (VW)	G - Medewerker bij VW	H - Extern e (niet-verwerker)
Collectief	① Privacybeleid	①	①	①	①		①		①
	② Convenant				②				
	③ Privacyreglement			③	③				③
	④ Verwerkersovereenkomst						④		
Indiv.	⑤ Geheimhoudingsverklaring	⑤			⑤	⑤			⑤
	⑥ Privacyprotocol	⑥	⑥		⑥	⑥			⑥

Documenten

1. In een *privacybeleid* staat wat de uitgangspunten inzake privacy zijn voor de gemeente. Dat moet kort, simpel en transparant verwoord zijn. Het is een publiek document (Internet/Intranet) dat voor een breed publiek toegankelijk moet zijn. Het beleid is intern en extern van toepassing. Voor burgers is het een statement, voor alle andere partijen bevat het bindende uitgangspunten voor samenwerking.
2. In een *convenant* wordt contractueel omschreven wat het doel van de overeenkomst is en wordt naar het privacyreglement verwezen voor welke regels er gelden m.b.t. de informatieveiligheid en in het verlengde daarvan de privacy.
3. In een *privacyreglement* staat verwoord wat de regels inzake privacy zijn waar partijen zich aan moeten houden. Het is een nadere uitwerking van het privacybeleid, concreet dus. Dat wordt strikt verwoord en heeft de status van openbaar reglement. Het is een onderlegger van elke overeenkomst met een externe samenwerkende partij die geen verwerker is.
4. In een *verwerkersovereenkomst* wordt contractueel omschreven hoe een externe partij met de verwerking van privacygevoelige informatie om moet gaan, wat het doel van de overeenkomst is en welke regels er gelden m.b.t. de informatieveiligheid en in het verlengde daarvan de privacy. Het bevat o.a. sancties.
5. In een *geheimhoudingsverklaring* wordt contractueel omschreven waar een persoon aan gehouden is m.b.t. geheimhouding en privacy. Het is de gepersonaliseerde versie van een reglement. Het bevat o.a. sancties.
6. In een *privacyprotocol* staan de gedragsregels voor personen die omgaan met privacygevoelige informatie. Als het privacyreglement of een convenant het 'Wat' omschrijft, dan gaat een protocol over het 'Hoe'.

Partijen (collectief) en Individuen

A. Een *externe medewerker* die onder direct gezag van de gemeente intern werkzaamheden verricht, zal als onderdeel van het contract met hem/haar of diens werkgever een individuele geheimhoudingsverklaring moeten ondertekenen. Daarbij wordt verwezen naar het privacybeleid (Internet/Intranet). Ter ondersteuning van de dagelijkse praktijk krijgt de externe ook het privacyprotocol overhandigd.

B. Een *medewerker* die onder direct gezag van de gemeente werkzaamheden verricht, legt de ambtseed af. Binnen de gemeentelijke CAO zijn de sancties vermeld die betrekking hebben op het schenden van de ambtseed. Dat dekt het formele aspect van geheimhouding. Daarnaast wordt verwezen naar het privacybeleid (Internet/Intranet). Ter ondersteuning van de dagelijkse praktijk krijgt de medewerker ook het privacyprotocol overhandigd.

C. Een *burger* zoekt naar houvast en transparantie over hoe de gemeente met informatieveiligheid en diens privacy omgaat. Dat staat helder verwoord in het privacybeleid. Ook wil hij weten wat de regels zijn, met name die hem aangaan over inlichten, bezwaren en klachten. Hier voorziet het privacyreglement in.

D. Een *samenwerkende instantie* trekt samen met de gemeente op in uitvoering van taken namens de gemeente. Dat betekent dat deze zoveel mogelijk gefaciliteerd moeten worden en dat de gemeente een extra verantwoordelijkheid heeft in het afdwingen van regels en protocollen op grond van haar eigen expertise en verantwoordelijk.

E. Het bovenstaande uit punt **D** strekt zich dan per definitie uit naar een *medewerker/vrijwilliger* bij de samenwerkende instantie, die daar taken uitvoert waarbij het in geding komen van de informatieveiligheid of privacy van burgers altijd de gemeente aangerekend zal worden.

F. Een *verwerker* is een professionele partij die namens de gemeente gegevens opslaat en mogelijk ook verwerkt. Hiertoe sluiten partijen een contract af, waarbij de informatieveiligheid en privacy voorzieningen die de verwerker treft in de verwerkersovereenkomst benoemd worden. Hierin staat o.a. dat een geheimhoudingsverklaring en privacyprotocol expliciet tot de interne verantwoordelijkheid van de verwerker horen.

G. Het bovenstaande uit punt **F** strekt zich dan per definitie uit naar een *medewerker* bij de *verwerker*, die daar taken uitvoert waarbij het in geding komen van de informatieveiligheid of privacy van burgers direct de verwerker contractueel aangerekend zal worden. De verwerker organiseert zichzelf op dit punt en is daarop contractueel aanspreekbaar.

H. Een *externe medewerker* die in opdracht van de gemeente extern werkzaamheden verricht, zal als onderdeel van het contract met hem/haar of diens werkgever een individuele geheimhoudingsverklaring moeten ondertekenen. Daarbij wordt verwezen naar het privacybeleid (Internet/Intranet). Ter ondersteuning van de dagelijkse praktijk krijgt de externe ook het privacyprotocol overhandigd.