Gemeente Kerkrade

GEMEENTEBLAD

Officiële uitgave van de gemeente Kerkrade

Nr. 136297

3 juni

2019

Privacy beleidskader

Verklaring van afkortingen

AVG Algemene Verordening Gegevensbescherming
Wbp Wet bescherming persoonsgegevens
AP Autoriteit Persoonsgegevens
FG Functionaris Gegevensbescherming
Awb Algemene wet bestuursrecht
BIG Baseline Informatiebeveiliging Nederlandse Gemeenten
College College van Burgemeester en Wethouders van gemeente Kerkrade
ENSIA Eenduidige Normatiek Single Information Audit
KCC Klant Contact Centrum van de gemeente Kerkrade
CISO Certified Information Security Officer
OESO Organisatie voor Economische Samenwerking en Ontwikkeling

Voorwoord
Voor u ligt het privacy beleidskader van de gemeente Kerkrade. Dit document is opgesteld naar aanleiding van de groeiende vraag vanuit zowel de organisatie als de wetgeving naar een verantwoord gebruik van persoonsgegevens van de inwoners van de gemeente. Het doel van dit beleidskader is om een stevige basis te leggen voor de bescherming van persoonsgegevens1, waarbij de nadruk ligt op de implementatie van privacy binnen de gemeentelijke organisatie middels generiek vastgestelde managementafspraken welke moeten worden nagekomen in alle gevallen dat persoonsgegevens worden verwerkt2. Bij het opstellen van dit privacy beleidskader is van de huidige heersende privacywet- en regelgeving gebruikt gemaakt als uitgangspunt, waarbij alle aspecten die van toepassing zijn op de gemeentelijke organisatie zijn uitgelicht.
Bij het schrijven van dit document is bewust getracht om de wetgeving niet letterlijk te kopiëren, maar dit te vertalen naar minder juridisch jargon. Op enkele punten bleken de wettelijke kaders echter dusdanig complex, dat bij de interpretaties die gedaan zijn een verwijzing naar het wetsartikel, waarop deze zijn gebaseerd, noodzakelijk werd geacht om toch een volledig beeld te geven.
Hoewel dit privacy beleidskader dient als praktisch handvat bij vraagstukken omtrent privacy en persoonsgegevensbescherming, is elke situatie waarin dit onderwerp aan bod komt anders. Het advies is dan ook om altijd de privacybeheerder binnen de specifieke sector/vakafdeling te raadplegen bij al dan niet complexe situaties.
Op basis van dit privacy beleidskader is een “privacy implementatieplan2018-2019 ” uitgewerkt waarin specifieke AVG verplichtingen aan bod komen en de jaarlijkse actiepunten concreet zijn beschreven om zo spoedig als mogelijk te komen tot een gemeentelijke bedrijfsvoering te komen die AVG proof is.
Opgemerkt moet wel worden dat beide documenten onderhevig kunnen zijn aan veranderingen, gelet op de voortvarende c.q. snelle ontwikkeling op het gebied van privacy. Aanbevolen wordt dan ook om periodiek (jaarlijks) een evaluatie uit te voeren en daar waar nodig aanpassingen te verrichten om de daadwerkelijke (jaarlijkse) actuele stand van zaken weer te geven.

Er is vertrouwen dat beide documenten als een gedegen basis dienen voor niet alleen het welslagen van de na te komen wettelijke verplichtingen, maar tevens voor een behoorlijke en terdege gemeentelijke dienstverlening, waarbij oog is voor de bescherming van de persoonlijk levenssfeer van de inwoners van de gemeente.

Leeswijzer
In het privacy beleidskader worden in navolging op de algemene uitgangspunten, aandacht besteedt aan de verantwoordelijkheden en het benodigde privacy management. De essentieel benodigde cultuurverandering en bewustwording komen aan bod in hoofdstuk 4 en in hoofdstuk 5 komen de operationele uitgangspunten aan bod. Naast de legitimiteit van verwerkingen, de mogelijke grondslagen voor een verwerkingsactiviteit en de vereiste transparantie hieromtrent, komen onder andere tevens pseudonimiseren, profilering en de rechten van betrokkenen, het proces(ontwerp-)plan en de meldplicht datalekken ter sprake. De planning & controll cyclus van privacy komt aan bod in hoofdstuk 6 en in hoofdstuk 7 worden de risico’s en gevolgen aangegeven indien het privacy beleidskader door de gemeentelijke organisatie niet wordt nageleefd.
Het onderwerp beveiliging heeft een eigen beleid, genaamd “informatiebeveiligingsbeleid”, waardoor er in dit privacy beleidskader enkel de samenhang tussen de onderwerpen wordt beschreven.

Inleiding

Gemeenten zijn, als verlengstuk van de Rijksoverheid, in Nederland verantwoordelijk voor het leveren van verschillende producten en diensten aan haar inwoners. Denk bijvoorbeeld aan het verstrekken van paspoorten en andere reisdocumenten, het registreren van partnerschappen, verhuizingen, geboortes, sterfgevallen, verstrekken van bijstandsuitkering etc. Bij het uitvoeren van deze publieke taken wordt gebruik gemaakt van een aantal (gewone, bijzondere en gevoelige) persoonsgegevens3 zoals bijvoorbeeld het Burger Service Nummer (voortaan: BSN) en de NAW-gegevens4. De persoonsgegevens worden gebruikt om de inwoner te identificeren en zijn dus herleidbaar naar die ene specifieke persoon.
Met de decentralisatie van de Rijksoverheid is het takenpakket van de gemeente steeds groter geworden. Onder andere het verlenen van de juiste zorg met behulp van externe partijen/derden en samenwerkings-/ketenpartners behoort tot de dagelijkse gemeentelijke dienstverlening. Om deze diensten te verlenen, vragen gemeenten de inwoners om steeds meer gegevens, zodat deze publieke taken uitgevoerd kunnen worden. Als gevolg hiervan komen gemeenten dan ook meer en meer in het bezit van velerlei gevoelige informatie, waarbij gedacht kan worden aan schuldindicaties, informatie over verslavingen, strafrechtelijke en/of medische gegevens etc.
Om deze persoonsgegevens zorgvuldig en behoorlijk te kunnen verwerken5, wordt intensief gebruik gemaakt van de laatste ontwikkelingen op het gebied van digitale dienstverlening. Waar enkele jaren geleden de persoonsgegevens nog (analoog) in archiefkasten werden bewaard, worden ze tegenwoordig steeds meer opgeslagen in en verwerkt door een grote variëteit aan digitale oplossingen. Dat deze digitale oplossingen bijdragen aan een goede en snelle dienstverlening is inmiddels gebleken. Echter, deze groei aan digitale oplossingen brengt ook een sterke groei aan risico's met zich mee.
De 'draagbaarheid' van persoonsgegevens op bijvoorbeeld mobiele apparaten, zoals IPads, laptops, smartphones en USB-sticks brengt een toename van risico's op beveiligingslekken/datalekken (met als doel gegevens buit te maken en te verkopen of gebruiken voor identiteitsfraude) met zich mee. Hierdoor komt bij het verwerken van persoonsgegevens de privacy van de betrokken burger in het geding. Buiten de wettelijke plicht een zorgvuldige en behoorlijke beveiliging van de persoonsgegevens te garanderen, hebben gemeenten ook de grondwettelijke plicht om bij voorbaat prudent om te gaan met de gevoelige informatie die burgers aanreiken. Immers hebben alle Nederlandse burgers volgens artikel 10 Grondwet "recht op eerbiediging en bescherming van de persoonlijke levenssfeer en menselijke waardigheid".

1. Juridisch kader

1.1 De Grondwet (GW)

Om de eerdergenoemde Grondwet terdege toe te kunnen passen op het gebruik van persoonsgegevens, kende Nederland vanaf 1989 de Wet persoonsregistratie. Deze wet werd in 2001 vervangen door de Wet Bescherming Persoonsgegevens (voortaan; Wbp)en was gebaseerd op de Europese Dataprotectierichtlijn (95/46/EG). Deze richtlijn gold voor alle Europese lidstaten en de nationale wet- en regelgevingen dienden hierop te worden gebaseerd, waarbij het de nationale lidstaten echter wel vrij stond om de kaders verdergaand naar eigen vrijheid in te vullen. Hierdoor ontstonden grote verschillen in de privacywetgeving tussen de Europese lidstaten.
Met de exponentiële groei van eerdergenoemde digitale oplossingen, waarbij landsgrenzen niet langer bindend waren, werd bij de Europese Unie de noodzaak erkend van een overkoepelende en gelijkluidende privacywetgeving voor alle Europese lidstaten.

1.2 Specifieke (materiële sectorale) wet- en regelgeving

De praktische uitwerking van de Wbp is voor de verschillende gemeentelijke domeinen vastgelegd in verschillende sectorale materiewetten, waarin de uitwisseling van persoonsgegevens voor de betreffende sectoren werd geregeld. Voorbeelden binnen het Sociaal Domein zijn de Wet werk en bijstand, Wet SUWI, Jeugdwet, Wet maatschappelijke ondersteuning, Wet publieke gezondheid, Algemene Wet Bijzondere Ziektekosten, Zorgverzekeringswet en de Wet gemeentelijke schuldhulpverlening en Leerplichtwet. Zie bijlage 1.
De uitwisseling van persoonsgegevens is echter ook vaak nader geregeld in een samenwerkingsverband, waarbij vaak een convenant een privacy protocol bevat. Dergelijke protocollen kunnen landelijk of voor een bepaalde beroepsgroep in overleg overeengekomen zijn, echter ook lokaal bij de afwezigheid van eerdergenoemde.

1.3 Meldplicht datalekken

Op 1 januari 2016 trad de wet "Meldplicht datalekken" in werking en werd deze opgenomen in de Wbp en recentelijk in de Europese Algemene Verordening Gegevensbescherming (voortaan: AVG). Het doel was en is de beperking van de schade bij betrokkenen in het geval van datalekken, waarbij de kans bestaat op verlies of onrechtmatige verwerking van de persoonsgegevens. De AVG stelt de verwerkingsverantwoordelijke verplicht om van een datalek melding te maken bij de Autoriteit

Persoonsgegevens (voortaan: AP). De AP mag na eigen beoordeling van de nalatigheid van de organisatie een bestuurlijke boete opleggen. Een dergelijke boete wordt uitgedeeld op basis van het incident, waardoor melding maken van het incident niet per definitie voldoet voor vrijwaring van onderzoek en eventuele beboeting door de AP.

1.4 De (Europese) Algemene Verordening Gegevensbescherming (AVG)
In 2016 trad de aldus de Europese Algemene Verordening Gegevensbescherming (voortaan; AVG) in werking ter vervanging van de eerdergenoemde privacyrichtlijn die niet meer aansloot op de actuele digitale oplossingen. Doordat het een Europese verordening is deze rechtstreeks van toepassing op alle Europese lidstaten en zijn gelijkwaardige nationale wetgevingen niet meer geldig. In de AVG zijn een aantal zaken veranderd ten opzichte van de Wbp, waaronder de rol van de toezichthoudende nationale autoriteit. Om organisaties (2 jaar de) tijd te gunnen hun bedrijfsvoering in te richten op deze nieuwe wetgeving, kreeg de AVG pas na 2 jaar (op 25 mei 2018) rechtstreekse werking.
In navolging van de AVG, waar ruimte aan lidstaten werd gelaten om enkele zaken zelf in te richten, stelde de Rijksoverheid een Uitvoeringswet Algemene Verordening Gegevensbescherming (voortaan: UAVG) op. Deze UAVG laat wetten uit de Wbp aansluiten bij de Europese AVG, waardoor de Wbp bij ingang van de uitvoeringswet niet meer geldig is.

1.5 Belangrijkste wijzigingen ten opzichte van de Wbp
Zoals eerder aangegeven traden door de invoering van de AVG enkele belangrijke wijzigen op per 25 mei 2018 ten opzicht van de Wbp. Onderstaand worden deze kort omschreven:
- Functionaris Gegevensbescherming (FG)6
De aanwijzing van een FG is niet langer vrijblijvend voor overheidsorganisaties, maar een verplichting. De FG is verantwoordelijk voor het naleven van de AVG binnen de organisatie en rapporteert direct aan de hoogst verantwoordelijke. De inbedding van een FG binnen de gemeente zal terugkomen in hoofdstuk 3.

- Rechtmatigheid en transparantie7
In de AVG is transparantie opgenomen als een apart beginsel. De transparantie heeft betrekking op de verzameling, het gebruik en verwerking van persoonsgegevens.
Het dient voor de betrokkene transparant te zijn in welke mate gegevens verzameld, gebruikt en verwerkt worden en op basis van welke wettelijke grondslag dit gebeurd.

- Accountability8
De gemeente zal actief beleid moeten voeren en maatregelen treffen waaruit blijkt dat de AVG wordt nageleefd. Een passieve informatievoorziening over het verwerken van persoonsgegevens is niet meer afdoende.

- Vergeetrecht9
Inwoners van de gemeente hebben het recht om ‘vergeten’ te worden, wat neerkomt op het recht om uit zowel analoge als digitale databases verwijderd te worden. Dit kan alleen gebeuren als er geen wettelijke eisten gesteld zijn aan de opslag c.q. het bewaren van persoonsgegevens.

- Dataportabiliteit10
Burgers hebben het recht om zijn of haar data mee te kunnen nemen naar een andere dienst. Tevens hebben ze het recht om een kopie te ontvangen van de persoonsgegevens die over hen zijn verzameld.

- Profilering11
In de AVG bestaat het recht voor inwoners van de gemeente om niet onderworpen te worden aan een besluit dat gebaseerd is op louter geautomatiseerde verwerking van persoonsgegevens. De meest voorkomende manier van deze manier van verwerken is profileren, waarbij grote hoeveelheden data worden verwerkt om een profiel te beoordelen. Deze manier van verwerking is niet toegestaan indien het de betrokkene in aanmerkelijke mate treft.

- Gegevensbescherming bij ontwerp of standaarden12
Anders dan voorheen wordt de nadruk gelegd op het treffen van passende technische en organisatorische maatregelen om gegevens te beschermen tijdens de verwerking. Essentieel in deze is dat gegevensverwerking tot strikt noodzakelijk beperkt wordt. Hiervoor is de standaard dat privacybescherming meegenomen wordt in het ontwerp van een verwerkingsactiviteiten.

2 Algemene uitgangspunten
2.1 Doel
Door de majeure veranderingen in wetgeving en het verscherpt toezicht door de AP hierop, is de bescherming van persoonsgegevens een aandachtsgebied voor de gemeente. Dit privacy beleidskader voorziet in de inbedding van privacy in de organisatie, zodat de gegevens van inwoners van de gemeente veilig behandeld worden. Het doel is om van bovenaf gemeentebreed een generieke privacy koers te

bepalen die leidend is voor de manier waarop de gemeentelijke organisatie omgaat met privacywetgeving. Er wordt aldus niet ingezoomd op detaillistische spelregels die kunnen gelden voor specifieke beleidsterreinen of afdelingen van de gemeente.
Voor zover dit wel van belang is, kunnen directeuren/afdelingshoofden via thema- c.q. domeinbeleid of via proces(ontwerp-)plannen (zie verder paragraaf 2.4) nadere invulling geven aan het privacy beleidskader. Tevens geeft het privacy beleidskader voldoende handvatten om op een behoorlijke en zorgvuldige manier om te gaan met het verwerken van persoonsgegevens.

2.2 Betrokken partijen
Het privacy beleidskader beschrijft op hoofdlijnen een aantal belangrijke aspecten die tegelijkertijd de uitgangspunten vormen voor een gemeentebreed c.q. generiek privacybeleid (kapstokbeleid) waaraan aldus later andere regelingen en/of specifiek thema- c.q. domeinbeleid kan worden opgehangen. Het privacy beleidskader is bindend voor een ieder die voor de gemeente werkzaam is of bestuurlijk (eind-)verantwoordelijk is. Het bevat managementafspraken tussen het college van Burgemeester en Wethouder (voortaan; college) en de directie/het management. Deze afspraken moeten worden nagekomen in alle gevallen dat persoonsgegevens worden verwerkt.

2.3 Ambitie
De gemeente levert een groot aantal diensten en producten ten behoeve van haar burgers. Om de gemeentelijke taken uit te voeren is het onontkoombaar dat er persoonlijke gegevens van de burgers worden gevraagd en in sommige gevallen worden gedeeld met andere instanties. Hierbij dient de gemeente de persoonlijke levenssfeer van haar inwoners continue te waarborgen. Het belangrijkste fundament voor de gemeentelijke dienstverlening is de vertrouwensband tussen de gemeente en haar burger. De burger mag en moet erop kunnen vertrouwen dat privacy en informatiebeveiliging hoge prioriteit hebben binnen de gemeente. Het is daarom van belang dat er binnen de gemeentelijke werkprocessen op een zorgvuldig, transparante en veilige manier met de persoonsgegevens van de inwoners en de medewerkers wordt omgegaan. Het belangrijkste uitgangspunt daarbij is het naleven van de AVG, waarin de bescherming van het recht op (informationele) privacy nadrukkelijk is uitgewerkt, en volledig en terdege uitvoering wordt gegeven aan dit privacy kaderbeleid.

De gemeente ambieert om transparant te communiceren over de wijze waarop zij omgaat met persoonsgegevens. Op deze manier kan het college op een professionele wijze verantwoording afleggen aan de gemeenteraad, de samenwerkings-/ketenpartners, de burgers etc. over de privacy bestendigheid van de gemeentelijke organisatie.

2.4 Visie
Het college:
1. Draagt verantwoordelijkheden op aan de algemeen directeur;
De zorg voor privacy is op grond van de AVG een wettelijke en bestuurlijke verantwoordelijkheid van het college . De uitvoering ervan is ambtelijk opgedragen aan de algemeen directeur. Het college13, de directie en het management sturen op privacy volgens de onderstaande aspecten van privacy management;
a. Een directeur/afdelingshoofd voert, als onderdeel van zijn verantwoordelijkheid, regie en houdt toezicht op zijn werkprocessen op basis van dit privacy beleidskader.
b. Bij nieuwe of gewijzigde werkprocessen en/of verwerkingsactiviteiten waaraan privacy risico's zijn verbonden hanteert de directeur/het afdelingshoofd een proces (ontwerp-)plan14.
c. Een proces (ontwerp-)plan is duidelijk, actueel, in overeenstemming met de werkelijkheid en wordt periodiek geëvalueerd15.
d. Binnen een werkproces worden persoonsgegevens louter verwerkt voor het realiseren van het procesdoel16.
e. Binnen een werkproces wordt geen informatie verwerkt die niet noodzakelijk is17.
f. Een proces(ontwerp-)plan benoemt technische en organisatorische waarborgen voor een zorgvuldige, eerlijke, veilige en betrouwbare persoonsgegevensverwerking18.
g. Een proces(ontwerp-)plan omvat eventuele opdrachten aan ketenpartners of interne uitvoerders en afspraken over het toezicht door de directeur/het afdelingshoofd met betrekking tot een goede uitvoering van de werkzaamheden.
h. Indien een betrokkene gebruik maakt van zijn/haar rechten op basis van de AVG zal de desbetreffende directeur/het afdelingshoofd oftewel de aangewezen privacybeheerder alle informatie dan wel medewerking verlenen aan de FG, zodat het verzoek van de betrokkene binnen de wettelijke termijn (1 maand) kan worden afgehandeld door de gemeente19.
i. Bij informatiebeveiligingsincidenten maakt de directeur/het afdelingshoofd gebruik van de centrale incidentmanagementprocedure die is uitgewerkt in het informatiebeveiligingsbeleid en bij een datalek van het protocol " Meldplicht van datalekken" inclusief bijbehorende gelijkluidende procedure.
j. Bij de aanpassing van een privacy risicovolle gegevensverwerking laat de directeur/het afdelingshoofd zich auditen door de FG aan de hand van de privacy kernpunten en zijn proces(ontwerp-)plan20.

2. Voorziet in een team van professionals (het Privacy Kernteam – privacybeheerders) dat het college, de algemeen directeur, de directeuren en de afdelingshoofden ondersteunt in de privacy beleidsuitvoering.
3. Voorziet in faciliteiten voor bewustwording en training21.
4. Treft maatregelen voor informatiebeveiligingsincidenten en mogelijk daaruit voortvloeiende datalekken22.
5. Evalueert om de drie jaren de doeltreffendheid en doelmatigheid van het privacy beleidskader23.
6. Informeert de raad over de privacy beleidsuitvoering24.
7. Handhaaft het privacy beleidskader. De gemeente wijst hiervoor een FG aan die toeziet op de borging van privacy binnen de gemeentelijke organisatie25.

2.5 Reikwijdte
Het Privacy beleidskader;
a. is van toepassing op de volledige gemeentelijke bedrijfsvoering, voor zover daarbij wordt gewerkt met persoonsgegevens en de gemeente ook zeggenschap heeft over de persoonsgegevens;
b. vormt het privacy beleidskader, in feite de kapstok, waaraan specifieker (thema c.q. deel-) beleid aan kan worden gehangen;
c. heeft invloed op alle interne processen, waarin persoonsgegevens worden verwerkt en op alle ondersteunende (afdelings-)applicaties voor informatieverwerking en gegevensopslag26. Daarbij is niet van belang of de informatieverwerking analoog (op papier) of digitaal plaatsvindt;
d. heeft invloed op alle externe processen die de gemeente uitbesteedt, inkoopt of op ander manier organiseert (samenwerkingsverband, Gemeenschappelijke Regeling, etc.);
e. heeft invloed op de gegevensuitwisseling met derden27, zoals gemeenten, de provincie, het rijk, de Belastingdienst, de politie, de Raad van Kinderbescherming, zorgaanbieders etc.
f. omvat de gehele "informatielevenscyclus"
Het verkrijgen / verzamelen van gegevens →het gebruiken van gegevens → het opslaan van gegevens → het archiveren van gegevens → het vernietigen van gegevens
g. is van toepassing op de verwerking van statische, wetenschappelijke versleutelde en geanonimiseerde gegevens, voor zover niet kan worden uitgesloten dat personen kunnen worden geïdentificeerd of geprofileerd.
h. in acht wordt genomen als er wordt gesproken over de persoonsgegevens van de medewerkers.
i. is van toepassing alle gegevens die herleidbaar zijn naar een natuurlijk persoon. Overleden personen zijn wettelijk geen natuurlijke personen, en dit beleid is dan ook niet op van toepassing is op hun gegevens.
j. over de verantwoordelijke spreekt en dat dit in alle gevallen een portefeuillehouder of de burgemeester van het college is, ongeacht de actuele mandaten. Dit wordt nader gespecificeerd in het privacy beleidskader zelf.

2.6 Raakvlak met informatiebeveiligingsbeleid
Het privacy beleidskader heeft verschillende raakvlakken met andere beleidsthema's of vertoont daarmee een overlap zoals integriteit, informatiebeveiliging, personeel en organisatie en communicatie. Van belang hierbij is dat de doelen van de privacywetgeving worden behaald. Veruit de grootste raakvlakken bestaan tussen privacy en informatiebeveiliging.
Om het onderscheid tussen privacy en informatiebeveiliging te benadrukken, worden de definities van de twee naast elkaar gelegd:
Privacy wordt kortweg ook wel omschreven als het recht om met rust te worden gelaten. Er zijn verschillende vormen van privacy, zo wordt bijvoorbeeld onderscheid gemaakt naar relationele, lichamelijke, territoriale, communicatieve, medische en informationele privacy. Deze dimensies geven invulling aan de persoonlijke levenssfeer. Eerbiediging van de persoonlijke levenssfeer is zoals reeds eerdergenoemd als grondrecht vastgelegd in artikel 10 van de Grondwet en richt zich op de informationele privacy en bestaat uitonderstaande achttal kernprincipes die gebaseerd zijn op de OESO privacy principes28;

1) Rechtmatigheid;
2) Datakwaliteit;
3) Doelbinding;
4) Dataminimalisatie;
5) Transparantie;
6) Rechten van betrokkene;
7) Accountability; en
8) Beveiligingsmaatregelen (informatiebeveiliging).
Vanuit het achtste kernprincipe wordt een bruggetje gemaakt met de technische IT-kant, namelijk informatiebeveiliging.
Informatiebeveiliging is het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van alle vormen

van informatie binnen een organisatie (of een maatschappij) garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.
Ook informatiebeveiliging heeft zijn eigen kernprincipes. De drie kernprincipes (BIV)van informatiebeveiliging luiden als volgt:
a) Beschikbaarheid (alle informatie moet te allen tijde beschikbaar zijn);
b) Integriteit (informatie moet betrouwbaar/correct zijn. Er mag niet getwijfeld worden aan de informatie); en
c) Vertrouwelijkheid (informatie beschermen tegen ongeautoriseerde toegang/inzage).
Kortweg kan gesteld worden dat informatiebeveiliging zich alleen bezighoudt met het daadwerkelijk (digitaal) beveiligen van opgeslagen informatie en dat privacy de focus legt op het legitiem verzamelen en gebruik van deze gegevens. Als eenmaal bepaald is dat er voldoende legitimiteit bestaat voor het verwerken van persoonsgegevens, is het verplicht hier ook de nodige passende en organisatorische beveiligingsmaatregelen voor te treffen. De officiële wettelijke richtlijn hiervoor is 'maatregelen voor een beveiligingsniveau dat afgestemd is op het risico dat de verwerking met zich meebrengt'. Om dit beveiligingsniveau te garanderen is de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) opgesteld door de Informatie Beveiligingsdienst. Deze baseline is opgesteld als richtlijnen voor voldoende waarborging van informatiebeveiliging binnen gemeentelijke organisaties. De gemeente heeft zich gecommitteerd aan de naleving van deze baseline.
Zowel de privacywetgeving als specifiek de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG) eisen dat de gemeente alle technische en organisatorische beveiligingsmaatregelen neemt om een op het risico afgestemd beveiligingsniveau te waarborgen. Welke beveiligingsmaatregelen dat precies (moeten) zijn, is nader uitgewerkt in het generieke informatiebeveiligingsbeleid van de gemeente. Dit beleid moet, net als het privacy beleidskader, gezien worden als een kapstok waaraan alles met informatiebeveiliging (kernprincipe a tot en met c) te maken heeft, is opgehangen.

Omdat de onderwerpen informatiebeveiliging en privacy dusdanig qua inhoud van elkaar verschillen, wordt informatiebeveiliging individueel geborgd binnen de gemeentelijke organisatie. Dit gebeurt middels informatiebeveiligingsbeleid en de rol van Chief Information Security Officer (voortaan; CISO).

3 Verantwoordelijkheden en privacy management

Er kan op het gebied van de verwerking van persoonsgegevens onduidelijkheid bestaan over de verantwoordelijkheid. Het is mogelijk dat dit leidt tot onwetendheid of onverschilligheid ten opzichte van de hierbij behorende verantwoordelijkheden. Dit hoofdstuk geeft inzicht in de verschillende niveaus hiervan.
Ook is persoonsgegevensdeling met en de verwerking ervan door externe partijen/derden steeds vaker in de praktijk aan de orde door de sterk opkomende digitalisatie. Door het vaststellen van verantwoordelijkheden hieromtrent is eenieder op de hoogte welke verantwoordelijkheid welke functie draagt en welke taken daarbij horen.

3.1 Politieke/bestuurlijke verantwoordelijkheid

Het sturen op privacy is wettelijke de taak van het college en is gekoppeld aan algemene beginselen van behoorlijk bestuur. Als dagelijkse bestuur is het college politiek eindverantwoordelijk voor de uitvoering van wettelijke regelingen en aldus ook de privacywetgeving. Het college draagt als hoogste organisatorisch orgaan zorg voor een behoorlijke en zorgvuldige persoonsgegevensverwerking die in overeenstemming is met de privacywetgeving en voert actief privacybeleid, waarbij rekening wordt gehouden met de afweging van de verschillende belangen en de risico's die horen bij de betreffende verwerking van persoonsgegevens.
Dit betekent dat het privacy beleidskader behoorlijk, zorgvuldig en in overeenstemming is met de wet29. Aanvullend legt het college over de privacy beleidsuitvoering verantwoording af aan de gemeenteraad en streeft transparantie hieromtrent na met behulp van communicatiemiddelen30.
Tevens draagt het college zorg voor de documentatie van beleid en uitvoeringsmaatregelen, zodat op ieder gewenst moment een juridische en maatschappelijke uitleg gegeven kan worden over de adequate en solide aanpak. Het college dient aldus aan te tonen (accountability) dat hun privacy management hieraan voldoet31. Indien dat niet lukt, loopt de gemeente maatschappelijke, politieke en juridische afbreukrisico's.
Het college stelt vervolgens een gemeentelijk register van de verwerkingsactiviteiten op (voortaan: GR) waarin alle werkprocessen met persoonsgegevens worden geregistreerd die onder zijn verantwoordelijkheid plaatsvinden, waarbij het register voldoet aan de voorwaarden uit artikel 30 AVG32. Zie verdergaand paragraaf 5.7. Elk collegelid is daarbij politiek verantwoordelijk voor de verwerking van persoonsgegevens die in zijn/haar portefeuille verwerkt worden.
Privacy valt onder de portefeuillehouder Financiën, Informatisering en automatisering, Publiekszaken en dienstverlening en Wijkwethouder Oost. Binnen het college is deze portefeuillehouder het vaste aanspreekpunt voor privacy aangelegenheden.

Het college wijst tevens een Functionaris voor Gegevensbescherming (voortaan: FG) aan als interne toezichthouder33. Deze adviseert en ondersteund tevens samen met een Privacy Kernteam (privacybeheerders) de directie/ de afdelingshoofden bij de uitvoering van het privacy beleidskader. De FG rapporteert rechtstreeks aan het college34. Zie verder paragraaf 3.4.

3.2 Ambtelijke verantwoordelijkheid

De taken die voortvloeien uit de verplichtingen en taken die de gemeente uitvoert, staan onder ambtelijke leiding van de algemeen directeur. Deze is aldus ambtelijk eindverantwoordelijk voor de correcte naleving van privacywetgeving en is samen met het Directieteam (DT) verantwoordelijk voor de inrichting en het aansturen van werkprocessen die in het GRV worden geregistreerd.
Door het feit dat privacy een rol speelt binnen deze taken en werkprocessen, is de directie van de gemeente ambtelijk verantwoordelijk voor de verwerking van de gegevens binnen hun sector. De uiteindelijke (politieke) eindverantwoordelijkheid ligt bij het college, maar van de directie wordt verwacht dat zij rekening houden met de alle aspecten van privacybescherming bij het aansturen op werkprocessen en de betreffende portefeuillehouder(-s) hierover informeren.

3.3 Operationele verantwoordelijkheid

De operationele verantwoordelijkheid ligt bij de directeuren samen met de afdelingshoofden. Zij dienen ervoor zorg te dragen dat de gemeentelijke taakuitoefening c.q. werkprocessen, inclusief de daarbij behorende verwerkingsactiviteiten, geschieden conform gestelde kaders zoals weergegeven in dit privacy beleidskader.
Het college verwacht van hen een rechtmatige en zorgvuldige verwerking van persoonsgegevens. De afdelingshoofden voerenregie over de afdelings-werkprocessen (verwerkingsactiviteiten) en zorgen voor een effectieve sturing op de uitvoering van deze. Het afdelingshoofd houdt tevens proactief toezicht op de privacy bestendigheid van zijn werkprocessen en legt keuzes en oplossingen op een begrijpelijke manier vast. Daarbij is de directie samen met de afdelingshoofden verantwoordelijk voor het vullen, controleren en wijzigen van het GRV conform artikel 30 AVG. Indien een gemeentelijke taakuitoefening op een dusdanige manier is ingeregeld dat de verwerkingsactiviteit inzake persoonsgegevens onder de operationele verantwoordelijkheid valt van meerdere afdelingshoofden, dan kan de algemeen directeur 1 afdelingshoofd aanwijzen die verantwoordelijk is voor deze gezamenlijke persoonsgegevensverwerking.
Ook bij een ieder die dagelijks gebruik maakt van eerdergenoemde ingerichte werkprocessen en daadwerkelijk de persoonsgegevens in (analoge als ook digitale) handen heeft. De werknemers zitten aan de bron van de verwerking en dragen elk zelf eveneens de verantwoordelijkheid dat alle persoonsgegevens verwerkt worden op de manier zoals voorgeschreven. Ook ligt bij de werknemers de verantwoordelijkheid om alle gegevens die ze onder ogen krijgen met de juiste mate van vertrouwelijkheid te behandelen en onregelmatigheden te signaleren.

3.4 Functionaris Gegevensbescherming

In essentie zorgt een Functionaris Gegevensbescherming (voortaan: FG) voor een goede uitvoering van het gemeentelijk privacybeleid en neemt daarbij een toezichthoudende en adviserende rol aan. Tot de kerntaak van de FG behoort het toezicht houden op en sturing geven aan op de later beschreven planning & control cyclus. De FG informeert en adviseert tevens onafhankelijk op alle echelons over de verplichtingen die de gemeente heeft volgens de AVG. Deze adviezen zijn niet bindend, maar wel zwaarwegend35. Bij een verschil van mening over het advies van de FG wordt aangeraden om dit expliciet vast te leggen waarom het advies van de FG niet is overgenomen.
In het kader van transparantie is de FG het officiële aanspreekpunt voor alle betrokkenen waarvan de persoonsgegevens worden verwerkt. Door de toezichthoudende, onafhankelijke rol van de FG kan er zonder belang bij de verwerking notitie gemaakt worden van klachten, vragen en andere aanverwante zaken.
De FG zal ook een officiële rol aannemen namens de gemeente jegens de AP. De FG treedt niet alleen op als contactpersoon, maar is ook verplicht om samen te werken met de AP. Om deze samenwerking te bevorderen is een officiële registratie bij de AP vereist. Deze registratie heeft als gevolg dat de FG opgenomen wordt in een openbaar register36. De aanmelding zorgt ervoor dat de FG genoteerd staat als contactpersoon en verlengstuk is van de AP. De aanmelding van de FG hoeft maar eenmalig te gebeuren en geschied middels een inschrijfformulier van de AP (bijlage 2). Uiteraard zal bij een functiewisseling een nieuwe aanmelding/inschrijving bij de AP moeten gebeuren.
Om te bepalen waar de FG geplaatst wordt binnen de gemeente wordt er enerzijds rekening gehouden met de wettelijke verplichtingen omtrent de positionering en anderzijds met een realistische, werkbare situatie voor de gemeente. Wettelijk zijn er bepaalde kaders aan de plaatsing van een FG binnen de organisatie gesteld. Deze zijn opgesteld om een goede bescherming van persoonsgegevens te kunnen garanderen. Zo handelt de FG op eigen initiatief en ontvangt geen instructies van het management, kan de FG niet worden ontslagen op basis van het uitvoeren van de gestelde taken (in het geval van onwenselijke meldingen) en behoudt de FG het recht om direct verslag uit te brengen aan de hoogst (eind-)verantwoordelijke voor de verwerkte persoonsgegevens37.
De middelen die een FG nodig heeft om te functioneren worden gefaciliteerd door het college. Hierbij kan gedacht worden aan;
- het door het bestuur en directieteam breed uitdragen van het belang om de FG te raadplegen;

- voldoende steun qua financiële en technische middelen
- het verlenen van de vereiste toegang/autorisaties zodat de FG onafhankelijk toezicht kan houden;
- het bieden van voldoende tijd om de FG te kunnen vervullen; en
- het bieden van (bij-)scholingsmogelijkheden om het kennisniveau op peil te houden.

De onafhankelijkheid van de functie FG wordt door het college vastgelegd door middel van een 'Regeling taken en bevoegdheden Functionaris Gegevensbescherming gemeente'. In deze regeling worden de wettelijke bevoegdheden en taken van de FG38 en een protocol melding onregelmatigheden vastgelegd. Tevens komen in deze regeling zaken zoals ontslagbescherming en geheimhoudingsplicht aan bod.

3.5 CISO

Het doel van de functie van Chief Information Security Officer (CISO) is om zorg te dragen voor een samenhangend pakket aan maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie binnen de organisatie. De exacte positie, taken en verantwoordelijkheden van de CISO worden specifiek in het informatiebeveiligings-beleid toegelicht, hieronder een kleine greep om de verschillen of overeenkomsten tussen CISO en FG aan te duiden:

- Optreden als beveiligingsadviseur bij (nieuwe) ICT –toepassingen;
- Initiëren of uitvoeren van periodieke kwetsbaarheidsanalyses;
- Zorg dragen voor bewustwording bij medewerkers; en
- Beveiligingsmaatregelen invoeren, handhaven of verbeteren.

3.6 Overlegstructuren

Om privacy door de hele gemeente in te bedden, wordt gebruik gemaakt van bepaalde overlegstructuren. Zo ligt in grote lijnen vast welke communicatielijnen er zijn betreffende de continue werkprocessen. Door regelmatig overleg te voeren kunnen strategische keuzes op lange termijn worden gemaakt, eventuele risico's eerder worden gesignaleerd, worden afdelingen specifiek betrokken bij privacyaspecten en wordt gezorgd voor een continue borging van privacy bewustwording. Zie bijlage 3.

Privacy kernteam

Bij de afdelingen wordt gebruik gemaakt van een 'privacybeheerder' genoemd. Deze beheerders zijn naast hun reguliere werkzaamheden extra geëngageerd met privacy binnen hun afdeling. Zie bijlage 4. Op deze manier wordt privacy dagelijks ingebed binnen de diverse werkprocessen, kunnen signalen eerder worden opgepikt en kan er sneller geanticipeerd worden op ad hoc situaties. De privacybeheerders nemen tevens deel aan een periodiek overleg dat wordt voorgezeten door de FG, het zogenaamde Privacy Kernteam. In deze overleggen kan elk lid agendapunten aandragen ter bespreking waarbij de andere leden als klankbord kunnen fungeren. Tevens wordt dit kernteam ad hoc ingeschakeld als er onverhoopt sprake is van een datalek.

Informatiebeveiliging

De FG zal periodiek in overleg gaan met de functies die verantwoordelijk gesteld zijn voor informatiebeveiliging binnen de gemeente, zoals de eerdergenoemde CISO. Aangezien privacy en informatiebeveiliging veel raakvlakken hebben dient het overleg ter afstemming van de gemeenschappelijke belangen en het te bepalen beleid hieromtrent. Uiteraard kan er gebruik worden gemaakt van wisselende samenstellingen als er sprake is van een vraagstuk binnen een specifiek domein.

4 Cultuur en bewustwording

De gemeente streeft een omgeving na waarbij persoonsgegevens op een rechtmatige en zorgvuldige manier verwerkt worden en privacy al wordt meegenomen in het ontwerp van een werkproces. Om dit te bewerkstelligen zal op zowel bestuurlijk als op ambtelijk niveau binnen de organisatie sprake moeten zijn van een bewuste omgang met gegevens in de werkprocessen. Dit bewustzijn richt zich vooral op de regels en gedragsnormen rondom privacy en informatiebeveiliging.

Naast deelname van de FG in de hoofdstuk 3 paragraaf 3.6 (zie bijlage 3) genoemde overlegstructuren, is de planning & control cyclus eveneens een middel om zowel te komen een tot gemeentelijke cultuur waarin privacy wordt gezien als een primair onderdeel van de gemeentelijke bedrijfsvoering, als tot stimulering van het privacy bewustzijn van de gemeente en haar medewerkers.

5 Operationele uitgangspunten

5.1 Legitimiteit van verwerkingsactiviteiten

Uitgangspunt bij het verwerken van persoonsgegevens is dat er geen ongelimiteerde verwerking plaatsvindt (dataminimalisatie), maar dat voor elke verwerking de legitimiteit getoetst wordt. De betrokkene heeft recht op een rechtmatige, behoorlijke en transparante wijze van verwerking van zijn of haar persoonsgegevens. Door bij elke nieuwe verwerking de legitimiteit van de verwerking mee te nemen in het ontwerpproces, wordt voldaan aan het principe 'gegevensbescherming bij ontwerp of standaarden'. Om dit recht te borgen dient voor elke verwerking rekening gehouden te worden met de volgende thema's;

5.1.1 Soorten persoonsgegevens

Als er gesproken wordt over persoonsgegevens, worden alle gegevens die herleidbaar zijn naar natuurlijke personen bedoeld. Hierbij kan er een onderscheid gemaakt worden tussen drie soorten. Gewone, bijzondere en identificerende (gevoelige) nummers. Deze classificatie is wettelijk bepaald en geeft een bepaalde zwaarte aan van deze gegevens.

Gewone persoonsgegevens staat in de wet vermeldt als elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon39. Hierbij kan gedacht worden aan naam, adres, woonplaats etc. De bepaling natuurlijke persoon houdt overigens in dat de gegevens van een overleden persoon géén persoonsgegevens zijn en dus verwerkt mogen worden.

Ook kan er sprake zijn van gevoelige persoonsgegevens. Deze genieten geen beschermde status, maar hebben een grotere impact op de persoonlijke levenssfeer dan reguliere persoonsgegevens. Dit zijn onder andere gegevens die:
- Betrekking hebben tot financiële of economische omstandigheden
- Kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, bijvoorbeeld informatie over verslaving, prestaties op school of relatieproblemen
- Betrekking hebben op inloggegevens
- Kunnen worden misbruikt voor (identiteits-)fraude zoals kopieën van paspoorten

Bijzondere persoonsgegevens zijn specifieke gegevens waar een wettelijk verbod op rust om deze te verwerken. De volgende gegevens worden onder deze categorie benoemd40:
- Ras of etnische afkomst
- Gezondheid
- Politieke gezindheid
- Godsdienst of levensovertuiging
- Lidmaatschap van een vakvereniging
- Genetische gegevens41 & Biometrische gegevens42
- Seksueel gedrag of seksuele gerichtheid

Voor een voorbeeldlijst van zowel gewone als bijzondere/gevoelige persoonsgegevens wordt verwezen naar bijlage 5.

Er zijn enkele situatie waarbij de wet het toelaat deze gegevens te gebruiken. Om te bepalen of er gebruik gemaakt mag worden van bijzondere persoonsgegevens kan de beslisboom in bijlage 6 gebruikt worden43. Als het verbod volgens de wet opgeheven kan worden, dient het persoonsgegeven op dezelfde manier behandeld te worden als een gewoon persoonsgegeven.

Een uitzondering op alle bovenstaande gegevens is een identificerend nummer. Onder een identificerend nummer wordt verstaan ‘een nummer dat ter identificatie van een persoon bij wet is voorgeschreven’. Een dergelijk nummer is bijvoorbeeld het Burger Service Nummer (voortaan: BSN). Het identificerend nummer mag uitsluitend worden verwerkt voor een wettelijk bepaalde doelstelling. Andersoortige verwerkingen zijn nadrukkelijk verboden.

5.1.2 Subsidiariteit, proportionaliteit en doelbinding
De persoonsgegevens van betrokkenen mogen niet verwerkt worden voor andere doelen dan waar ze origineel voor verzameld zijn. Praktisch houdt dit principe in dat voor elke verwerking opnieuw de gegevens opgevraagd moeten worden bij de burgers. Met het oog op de dienstverlening naar de burger zal dit niet keer op keer hoeven te gebeuren, mits de verwerking voldoende beargumenteerd is door de rest van deze thema’s.
Het principe van proportionaliteit behoedt de betrokkene van een ongelimiteerde verzameling van zijn of haar persoonsgegevens. De gemeente draagt zorg dat het doel van de verwerking niet onevenredig is aan het belang van haar burgers. Algemeen gesproken kan gezegd worden dat de gemeente niet meer gegevens verwerkt dat ze daadwerkelijk nodig heeft voor het vastgestelde doel.
De AVG schrijft voor dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld44. Welbepaald houdt concreet in dat men geen gegevens mag verzamelen voor onduidelijke of vage redenen. Uitdrukkelijk omschreven geeft aan dat het doel van verwerking voorafgaand in kaart gebracht dient te worden. Het verzamelen van de gegevens van willekeurige inwoners van de gemeente voor een doel dat mogelijk in de toekomst relevant kan zijn, is dus niet toegestaan.

5.2 Grondslagen voor verwerkingsactiviteiten

5.2.1 De 6 grondslagen
De AVG beschrijft op basis van welke grondslag gegevens verzameld mogen worden van betrokkenen. Deze geeft aan dat persoonsgegevens slechts verwerkt mogen worden indien:

a. De betrokkene zijn toestemming verleend heeft;
b. De verwerking expliciet noodzakelijk is voor het sluiten van een overeenkomst;
c. De verwerking noodzakelijk is voor een wettelijke verplichting;
d. De verwerking noodzakelijk is voor het vitaal belang van de betrokkene; en/of
e. De verwerking noodzakelijk is voor een goede vervulling van een taak van algemeen belang of openbaar gezag door de gemeente45.
Zie tevens bijlage 7.
De meest toepasbare grondslagen voor gegevensverwerking zijn sub c en e. De wettelijke verplichtingen en publiekrechtelijke taken vloeien voort uit sectorale wetgevingen, regelingen of richtlijnen. In het sociale domein kan hierbij vooral gedacht worden aan de wetten genoemd in bijlage 1.

Onderstaand wordt een handige beslisboom weergegeven om te kunnen beoordelen of persoonsgegevens verwerkt mogen worden:

5.2.2 Toestemmingsverklaring
Zoals bij de wettelijk grondslagen genoemd, mogen gegevens verwerkt worden als er toestemming door de betrokkene is verleend. Deze toestemming berust op de volgende voorwaarden;
- Toestemming wordt op een begrijpelijke, makkelijke en toegankelijke manier gevraagd;
- De betrokkene heeft te allen tijde het recht de toestemming weer in te trekken;
- De toestemming is vrijelijk en zonder dwang gegeven;

Uit onderzoek van de AP46 blijkt dat veel gemeenten een toestemmingsverklaring gebruiken als grondslag voor verwerking binnen het sociaal domein47. Na dit onderzoek is de AP echter tot de conclusie gekomen dat de toestemmingsverklaring als grondslag voor de verwerking niet voldoet aan de bovenstaande criteria.

Volgens de AP is er namelijk geen sprake van vrijelijke toestemming, daar er een afhankelijkheidsrelatie bestaat tussen de inwoner en de gemeente. Er kan bij diensten die de gemeente verleent aldus geen sprake zijn van een toestemmingsverklaring als grondslag voor gegevensverwerking. Deze wettelijke grondslag zal uit een van de sectorale wetten moeten voortvloeien.

Mocht in uitzonderlijke gevallen voor de gegevensdeling géén wettelijke grondslag bestaan, dan is een toestemmingsverklaring alsnog mogelijk onder eerdergenoemde voorwaarden.

5.2.3 Documentatieplicht

Om transparantie naar de betrokkenen te kunnen voeren is de gemeente verplicht een register bij de houden met alle verwerkingactiviteiten van persoonsgegevens. De oude meldplicht onder de Wbp is komen te vervallen door het uitgangspunt dat elke overheid met een FG een privacy specialist in dienst heeft en deze in staat is de hiermee gemoeide aspecten te beoordelen.
De verplichting om verwerking van persoonsgegevens te documenteren blijft dus wel bestaan. De gemeente dient dan nu ook zelf een register bij te houden van alle verwerkingsactiviteiten met persoonsgegevens dat wordt beheerd door de FG. Dit register houdt van alle verwerkingsactiviteiten, maar is niet gelimiteerd tot, de gegevens bij zoals opgenomen in het artikel 30 AVG-formulier van bijlage 8. De directeur/ het afdelingshoofd/ de privacybeheerder/privacycoördinator zorgt voor het invullen van dit artikel 30 AVG-formulier in het begin van een verwerkingsactiviteit, aldus bij het opstellen van een proces(ontwerp-)plan, oftewel bij een wijziging daarvan. Tevens wordt een afschrift van dit formulier aan de FG verstrekt ter registratie in het GRV conform artikel 30 AVG. Zie tevens hoofdstuk 3 paragraaf 3.3.
Wanneer een betrokkene inzage wilt hebben in zijn/haar persoonsgegevens, kan deze informatie opgevraagd worden uit dit document bij de FG.

5.3 Transparantie

5.3.1 Informatieplicht

De gemeente is wettelijk verplicht haar burgers te informeren over de rechten die ze hebben omtrent de verzameling van hun gegevens48. Dit houdt niet in dat er passief op basis van vragen informatie verstrekt wordt, maar dat een actieve informatievoorziening wordt gehandhaafd. Over de volgende zaken moeten betrokkenen minimaal door de gemeente worden geïnformeerd49 ;
- Dat het college verantwoordelijk is voor de verwerking van de persoonsgegevens, met bijbehorende contactgegevens;
- De contactgegevens van de FG;
- De verwerkingsdoeleinden van waarvoor de gegevens zijn bestemd en de wettelijke grondslag hiervan;
- De belangen van de gemeente bij het verzamelen van de persoonsgegevens
- Welke instanties toegang krijgen tot de persoonsgegevens;
- Hoelang de gegevens bewaard blijven, minstens de criteria waaraan de bewaartermijn moet voldoen;
- Dat de burger het recht tot inzage heeft;
- Dat de burger het recht op intrekken van toestemming heeft;
- Dat de burger het recht heeft om een klacht in te dienen bij de AP; en
- Het bestaan van geautomatiseerde besluitvorming indien dit toepasbaar is.

Deze informatie wordt zowel globaal als specifiek aangeboden aan de inwoners van de gemeente. Dit houdt in dat er op de eerste plaats ruimte is voor algemene informatievoorziening voor elke burger. Verder worden de burgers die gebruik maken van de producten en diensten van de verschillende domeinen (zoals bijvoorbeeld in het sociaal domein over de verlening zorg etc.) specifiek geïnformeerd over de verwerking van hun gegevens. De manieren van communiceren kunnen zijn, maar zijn niet gelimiteerd tot:
- Digitaal, door het beschikbaar maken van de informatie op de website
- Analoog, door het beschikbaar maken van de informatie op een flyer
- Mondeling, door de informatie toe te lichten tijdens contactmomenten

5.3.2 Verwerking en gegevensdeling met derden

In de doelstelling de burger zo efficiënt mogelijk te helpen, zijn veel diensten ondergebracht bij externe partijen/derden die IT-oplossingen aanbieden om verwerkingen door te voeren. Bij de meeste van deze diensten die persoonsgegevens verwerken, worden de persoonsgegevens aangeleverd en opgeslagen op servers van bijvoorbeeld een softwareaanbieder, waardoor deze conform privacywetgeving gekwalificeerd dient te worden als ‘verwerker’50.
In de wetgeving wordt duidelijk onderscheid gemaakt tussen de verwerker en verwerkingsverantwoordelijke. In de relatie tussen eerdergenoemde softwareaanbieder en gemeente is laatstgenoemde te allen tijde de verwerkingsverantwoordelijke. Dit houdt in dat er in de overeenkomsten met deze verwerker essentiële afspraken gemaakt moeten worden over de verwerking van de persoonsgegevens. Voor de bescherming van de persoonsgegevens is in elk geval essentieel dat de verwerker :
- Afdoende technische en organisatorische maatregelen biedt zodat er wordt voldaan aan de wettelijke verplichtingen van de privacywet met toepassing op de verwerker en de rechten van de betrokkene beschermd worden;
- Geen andere verwerker in dienst neemt zonder expliciete toestemming van de verwerkingsverantwoordelijke;
- Uitsluitend de gegevens verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke;
- Vertrouwelijkheid van persoonsgegevens in acht neemt;
- De verwerking beveiligd zoals omschreven in de privacywetgeving51;
- Na afloop van de overeengekomen diensten de gegevens teruggeeft aan de verantwoordelijke en dat bestaande kopieën verwijderd; en

- Alle informatie ter beschikking stelt als de verwerkingsverantwoordelijke hierom vraagt voor onder andere inspectiedoeleinden.
Bovenstaande informatie is niet limitatief en moet altijd specifiek aangepast worden op elke overeenkomst die aan de orde is. De verwerkersovereenkomsten worden altijd in overleg met de FG geaccordeerd, zodat deze acht kan nemen van de verwerking. Sjablonen voor modelovereenkomsten worden verstrekt door het KwaliteitsInstituut Nederlandse Gemeenten (KING).
De gemeente maakt bovendien gebruik van de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT). Deze inkoopvoorwaarden voor IT zijn opgesteld om een uniforme positie met alle gemeenten in te nemen ten opzichte van leveranciers. In deze inkoopvoorwaarden zijn alle heersende wet- en regelgevingen meegenomen. Er is dus al zekerheid dat de bovengenoemde zaken geborgd zijn in nieuwe contracten. Inzake de reeds bestaande contracten zal een AVG- herijking moeten plaatsvinden in overleg met de externe partij/derde.
De gemeente houdt ook het recht om een verwerker te controleren op een correcte naleving van eerdergenoemde verplichtingen. De gemeente blijft immers verantwoordelijk voor de gegevens. De controle kan uitgevoerd worden door een werknemer van de gemeente of door een gemachtigd externe controleur. Indien er besloten wordt dat een dergelijke controle wordt uitgevoerd, is de verwerker verplicht medewerking te verlenen en alle gewenste informatie te verstrekken52.
Aan een burger die gebruik maakt van zijn rechten dient te allen tijde de verwerkingen die door externe partijen/ derden plaatsvinden eveneens te worden betrokken. Zo heeft een burger immers het recht om te weten (transparantiebeginsel) waar en door wie en met welk doel zijn of haar gegevens worden verwerkt.

5.4 Pseudonimiseren en anonimiseren

Om het gebruik van persoonsgegevens te minimaliseren zijn er mogelijkheden om deze te versleutelen voor ze worden ontvangen door de verwerkers. Twee manieren om dat te bewerkstelligen zijn pseudonimiseren en anonimiseren.
Bij pseudonimisering worden de identificeerbare gegevens vervangen door versleutelde gegevens door middel van een algoritme. Op deze manier zijn de gegevens niet meer herleidbaar, maar kunnen deze wel in verschillende situaties aan elkaar gekoppeld worden indien het doel dit vereist. Dit proces is, mits de juiste beveiligingsmaatregelen worden gebruikt, omkeerbaar. Door de omkeerbaarheid van dit proces, blijft de privacywetgeving van kracht.
Zoals omschreven bij de soorten persoonsgegevens in hoofdstuk 5 paragraaf 5.1.1 mogen identificerende nummers niet verwerkt worden voor een doel dat niet wettelijk is voorgeschreven. Het pseudonimiseren van een BSN is dan ook verboden, daar de wetgeving van kracht blijft op deze gegevens.
Bij anonimiseren worden de identificeerbare gegevens verwisseld naar non-identificeerbare, willekeurige gegevens. Voorwaarde bij dit proces is dat de actie onomkeerbaar moet zijn, dus dat de anonieme gegevens nooit meer te herleiden zijn naar de betrokkene. Bij anonimiseren is de privacywetgeving niet meer van toepassing.
Het voordeel van de pseudonimisering is dat verschillende gegevens aan elkaar gekoppeld kunnen worden door hetzelfde algoritme, maar de privacywetgeving blijft van toepassing. Dit is anders bij anonimiseren, waarbij de privacywetgeving aldus niet meer van toepassing is.

5.5 Profilering

Profilering houdt in het verzamelen, analyseren en combineren van (persoons)gegevens met als doel iemand in te delen in een bepaalde categorie. Met profilering kan een organisatie ook het gedrag van mensen voorspellen of een beslissing over hen nemen. Profilering wil dus zeggen dat iemand aan de hand van een (risico)profiel wordt beoordeeld. Het proces van profilering bestaat uit drie stappen:
1. Het verzamelen van (persoons-)gegevens over (een groep) mensen
2. Het analyseren en combineren van deze, en soms ook andere, gegevens om verbanden en patronen te ontdekken
3. Het toepassen van de verbanden en patronen (profielen) op (een groep) mensen om hen in te delen in een bepaalde categorie en/of hun gedrag te voorspellen.

Als blijkt dat een verwerking aan de hand van deze stappen uitgevoerd wordt, is sprake is van profilering. Dan dienen de volgende punten schriftelijk vastgelegd en uitgevoerd te worden:

- Actieve informatievoorziening. De burger moet actief geïnformeerd worden over het bestaan van de profilering en de gevolgen daarvan;
- Recht op inzage. De burger kan te allen tijde opvragen welke gegevens worden gebruikt voor welk doel en wat de gevolgen daarvan zijn;
- De burger heeft het recht niet te worden onderworpen aan profilering en kan een verzet aantekenen tot het stopzetten van de gegevensdeling;
- Logica. De logica die ten grondslag ligt aan de (automatische) voorspelling moet in kaart gebracht zijn; en

- Geautomatiseerde systemen mogen alleen als hulpmiddel dienen. Beslissingen op basis van profilering moeten altijd genomen worden door een natuurlijk persoon.

Als er nadrukkelijk sprake is van een overeenkomst tussen gemeente en burger, toestemming is gegeven of sprake is van een wettelijke verplichting ter bescherming van de burger, is profilering toegestaan. Hierbij dient proportionaliteit goed in ogenschouw gehouden te worden. Bij het profileren van inwoners op basis van hun persoonsgegevens zijn een aantal risico's te benoemen. Deze zijn terug te vinden in hoofdstuk 7.

5.6 Rechten van betrokkenen
Betrokkenen hebben het recht op een rechtmatige en noodzakelijke handelswijze inzake hun eigen persoonsgegevens die in overeenstemming is met de het privacy beleidskader, waarbij de gemeente hen te allen tijde informatie over de doelen van een verwerkingsactiviteit en over privacy beleidsuitvoering (tranparantiebeginsel)53 kan verstrekken. Om betrokkenen ook daadwerkelijk regie te geven over hun eigen persoonsgegevens hebben zij onderstaande rechten die zij kunnen inroepen tegenover de gemeente en waarop de gemeente uiterlijk binnen 1 maand dient te reageren middels een besluit in de zin van de Awb 54. Zie bijlage 9.

5.6.1 Recht op inzage55
Als er sprake is van de verwerking van persoonsgegevens, is wettelijk vastgesteld dat de burger een verzoek tot inzage bij de gemeente kan indienen inzake zijn eigen persoonsgegevens. De informatie uit bijlage 9.1 moet dan binnen één maand verstrekt worden. De verstrekking hiervan moet kosteloos gebeuren, wanneer het verzoek in alle redelijkheid wordt gedaan. Dit betekent dat bij aanvragen met een 'buitensporig repetitief karakter' de gemeente de keuze heeft om administratiekosten voor het verzoek te vragen of het verzoek te weigeren.

5.6.2 Recht op rectificatie56
Betrokkenen hebben het recht op rectificatie van onjuiste persoonsgegevens. Bij het blijken van onvolledige informatie, kan dit door onder meer een aanvullende verklaring vervolledigd worden.

5.6.3 Recht op vergetelheid57
Wanneer gegevens verwerkt worden, hebben betrokkenen in sommige gevallen het 'recht om vergeten te worden'. Dit houdt in dat de gemeente verplicht is alle aangeduide persoonsgegevens te wissen wanneer een inwoner hierom vraagt, waarbij wel rekening dient te worden gehouden met de wettelijke bewaartermijnen. Naast de gegevens die in eigen beheer zijn, neemt de gemeente de taak om elke koppeling naar, of kopie van die gegevens te wissen. Als er beroep gedaan wordt op de dit recht, zijn de criteria in bijlage 9.2 van toepassing.

5.6.4 Recht op beperking58
De inwoners van de gemeente hebben het recht op beperking van de verwerking van hun persoonsgegevens. De beperking van de verwerking berust op de criteria genoemd in bijlage 9.3. Wanneer de beperking gegrond is, worden de gegevens alleen verwerkt met toestemming van de betrokkene, in geval van een rechtsvordering of voor een gewichtige reden van algemeen nationaal belang.

5.6.5 Recht op overdraagbaarheid59
Inwoners van de gemeente hebben het recht om de door hen aangeleverde persoonsgegevens 'mee te nemen' naar een andere dienst waar deze gegevens voor nodig zijn. Dit kan enkel in de gevallen waar de betrokkene zelf toestemming heeft gegeven voor verwerking, de verwerking vastgelegd is in een overeenkomst of de gegevens geautomatiseerd verwerkt worden. Wanneer een dergelijk verzoek ingediend wordt, moet de overdracht voldoen aan de criteria genoemd in bijlage 9.4.

5.6.6 Recht van bezwaar60
Het recht op bezwaar stelt de inwoners van de gemeente in de gelegenheid om bezwaar te maken tegen gegevensverwerking door de gemeente. Dit bezwaar kan ingediend worden op basis van een specifiek situatie van de burger die verband houdt met de verwerking. Wanneer een dergelijk verzoek ingediend wordt, staakt de gemeente onmiddellijk de verwerking. De verwerking hoeft niet gestaakt te worden wanneer de gegevens verwerkt worden op basis van dwingende gerechtvaardigde gronden die zwaarder wegen dan de belangen van de burger of de verwerking nodig is voor een rechtsvordering.

5.6.7 Recht op onthouding van automatische besluitvorming61
Wanneer er sprake is van automatische besluitvorming, waaronder profilering, heeft elke burger het recht om niet onderworpen te worden hieraan. Dit geldt niet wanneer deze verwerking nadrukkelijk

overeengekomen is in een contract of toestemmingsverklaring, of wanneer de verwerking specifiek wettelijk is toegestaan.

5.7 Gegevensbescherming bij ontwerp/standaarden

5.7.1 De GegevensEffectBeoordeling (GEB)
Bij bepaalde gemeentelijke werkprocessen waarin persoonsgegevens verwerkt worden, is een zogeheten 'gegevenseffectbeoordeling' (voortaan: GEB) verplicht62 . Een dergelijke beoordeling heeft als doelt te bepalen welke beveiligings- en of beheersmaatregelen passend en noodzakelijk zijn. Een GEB maakt gebruik van een vooropgestelde vragenlijst op basis waarvan de mate waarin en de manier waarop een werkproces, en de daarmee samenhangende persoonsgegevens-verwerkingsactiviteit, aandacht behoeft.

Door de risico's reeds in de ontwerpfase in kaart te brengen, kan eerder (en meestal goedkoper) bijgestuurd worden op risicovolle aspecten. De uitkomsten van een GEB worden weergegeven in een GEB-rapport dat wordt toegevoegd aan het in paragraaf 5.1 genoemde GRV. Een GEB is niet alleen van toepassing op concrete processen, maar ook op beleid, uitvoering en systematiek.

Elke proceseigenaar (directeur) is verantwoordelijk om een GEB uit te (laten) voeren bij de ontwikkeling/start van een verwerkingsactiviteit, maar is verplicht hierbij de privacybeheerder te raadplegen. Deze kan operationeel samen met de procesverantwoordelijke (afdelingshoofd) een GEB uitvoeren en adviserend optreden.

Pas nadat de verwerking in het GRV mag de verwerking van persoonsgegevens doorgang vinden c.q. starten!
Indien er aanpassingen nodig zijn in het proces om te voldoen aan de privacywetgeving is de proceseigenaar (directeur) verantwoordelijk voor de juiste aanpassingen alvorens het werkproces operationeel wordt. Wanneer blijkt dat een werkproces een hoog en onvermijdelijk risico met zich meebrengt en besloten wordt deze operationeel te laten worden kan het tevens verplicht zijn de AP het werkproces voor te leggen ter raadpleging. Deze zal vervolgens onderzoek doen naar de voorgestelde verwerking voorafgaand operationalisering. Een GEB moet in elk geval de volgende informatie bevatten:
- Een systematische beschrijving van de beoogde verwerkingen en de doeleinden;
- Beoordeling van de noodzaak en de evenredigheid;
- Beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
- Beoogde maatregelen om deze risico's aan te pakken.

Veel voorkomend is een GEB aan de hand van een vragenlijst. Er zijn diverse sjablonen beschikbaar voor dergelijke assessments, waarbij vooralsnog de vragenlijst van NOREA (It-auditor) als meest compleet ervaren wordt. Het is aan de FG om een actueel format voor deze effectbeoordelingen intern aan te bevelen.

Ten behoeve van een eenduidige systematiek past de gemeente echter wel een generieke werkwijze toe van positieve en negatieve GEB-scores. Hoe hoger de GEB-score hoe aanvullender de privacy- en informatiebeveiligingswaarborgen moeten zijn. Het afdelingshoofd volgt de GEB-score die door de privacybeheerder is vastgesteld. Een GEB-score wordt bepaald aan de hand van de onderstaande matrix:
Het bepalen van de GEB-score:
Bestuurlijke impact

C Hoog
B Midden
A Laag

C1	C2	C3
B1	B2	B3
A1	A2	A3

Persoonlijke impact
1- Laag 2-Midden 3-Hoog
De directeur/ het afdelingshoofd is bekend met zijn GEB-score en hanteert onderstaande tabel in hoeverre de GEB deel uitmaakt van het proces (ontwerp-) plan om op die manier de keuze(s) voor de privacy- en informatiebeveiligingswaarborgen te bepalen.

5.7.2 GEB-score in relatie tot het proces(ontwerp-)plan:

GEB- Score	Beheersmaatregelen	Samenspraak Privacybeheerder	Samenspraak FG

		/Privacycoördinator en evt. in Kernteam	
A1	n.v.t.	n.v.t.	n.v.t.
A2	Ja	Ja	Aanbevolen
A3	Ja	Ja	Ja
B1	Ja	Ja	n.v.t.
B2	Ja	Ja	Aanbevolen
B3	Ja	Ja	Ja
C1	Ja	Ja	Aanbevolen
C2	Ja	Ja	Aanbevolen
C3	Ja	Ja	Ja

Een GEB-rapport wordt door het afdelingshoofd opgesteld op basis van artikel 35 lid 7 AVG. Dit betekent dat het GEB-rapport ten minste moet bevatten:

- een systematische beschrijving van de beoogde persoonsgegevensverwerking en de verwerkingsdoeleinden;
- een beoordeling van de noodzaak en evenredigheid van de persoonsgegevensverwerking ten opzichte van de doeleinden;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkene(n), en
- de beoogde maatregelen om risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan de AVG is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkene(n) en andere personen in kwestie.

Het afdelingshoofd documenteert met behulp van het proces-(ontwerp-)plan hoe er op een praktische manier in passende organisatorische en technische privacy- en informatiebeveiligingswaarborgen wordt voorzien. Voornamelijk om de volgende fouten te voorkomen:

- Onrechtmatige persoonsgegevensverwerking: gebruik, opslag of uitwisseling van informatie is bij wet beperkt of zelfs verboden;
- Verwerken van persoonsgegevens door een verwerker zonder verwerkersovereenkomst: de verwerking van persoonsgegevens wordt uitgevoerd door een verwerker (externe partij) zonder dat er een verwerkersovereenkomst is afgesloten. Daardoor zijn er geen nadere afspraken gemaakt over: onderwerp, duur, aard, doel, soort persoonsgegevens, beveiligingsmaatregelen, geheimhouding, aansprakelijkheidsstelling, datalekmeldingen, rechten van de betrokkene(n), beëindigingmogelijkheden, audits etc.;
- Disproportionele persoonsgegevensverwerking: gebruik, opslag of uitwisseling van informatie is (a) ontoereikend of juist overmatig of (b) het gemeentelijk belang bij de gegevensverwerking is onevenredig klein terwijl de impact op personen onevenredig nadelig kan uitpakken;
- Niet-noodzakelijke gegevensverwerking: de gebruikte, opgeslagen of uitgewisselde informatie dient geen enkel gemeentelijk doel (meer), doet er niet toe of is sterk verouderd;
- Onnauwkeurige gegevensverwerking: de gebruikte, opgeslagen of uitgewisselde informatie is geen juiste weergave van de werkelijkheid;
- Onveilige gegevensverwerking: de gebruikte, opgeslagen of uitgewisselde informatie dreigt te gemakkelijk toegankelijk te zijn voor onbevoegden of ongeautoriseerden, gemanipuleerd te worden of niet beschikbaar te zijn; en
- Onbewaakte gegevensverwerking: het afdelingshoofd verzuimt om te controleren of de privacy waarborgen daadwerkelijk zijn geëffectueerd.

De werkelijkheid dient in overeenstemming te zijn met het proces (ontwerp-)plan. Veranderingen in het werkproces en de daarmee samenhangende persoonsgegevensverwerking verlangen dat het proces(ontwerp-)plan wordt aangepast. Dit betekent dat opnieuw een GEB moet worden uitgevoerd. Hierbij kan bijvoorbeeld gedacht worden aan wijzigingen van een bepaald (gedeelte) werkproces door gebruik te maken van nieuwe technologie.

5.8 Meldplicht datalekken

Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn aldus vastgelegd in de AVG. Zo is bepaald dat de verantwoordelijke voor deze verwerking van persoonsgegevens, meestal het college, maatregelen dient te treffen die verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens moeten voorkomen63.
Een datalek moet binnen 72 uren worden gemeld aan de AP via een online formulier64 als het leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of

als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het datalek moet daarnaast ook worden gemeld aan de betrokkene(-n) indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer65 .

Mocht besloten worden om de betrokkene(-n) niet te informeren, dan kan de AP alsnog na een onderzoek hiertoe verplichten. Als bepaald is om de
betrokkene(-n) te informeren, dient de informatie in elk geval te bevatten:

- Duidelijke en eenvoudige taal66;
- Omschrijving van de aard van de inbreuk;
- De naam en contactgegevens van de Functionaris Gegevensbescherming of ander contractpunt waar meer informatie kan worden verkregen67;
- De waarschijnlijke gevolgen van de inbreuk68:
- Eventueel te treffen maatregelen die de betrokkene wordt aanbevolen om negatieve gevolgen van de inbreuk te beperken69;
- Bij het beschrijven van de aard van de inbreuk kan doorgaans volstaan worden met een algemene omschrijving.
- Voorts wordt hierbij de contactgegevens opgenomen zodat de betrokkene terecht kan indien hij/zij vragen heeft over het datalek.
- Verder kan aangegeven worden wat de betrokkene zelf kan doen om de negatieve gevolgen van het datalek te beperken.

Om alle criteria mee te nemen en te bepalen of er in beginsel sprake is van een datalek en of de AP of de betrokkene(-n) dient/dienen te worden geïnformeerd kan de beslisboom in bijlage 10 worden gebruikt. Bij de eerste stap wordt bekeken of er sprake is van een inbreuk op de beveiliging. Dit hoeft niet per definitie te betekenen dat de beveiliging tekort is geschoten. Voorbeelden hiervan zijn het omzeilen van beveiligingsmaatregelen door bijvoorbeeld een hack of diefstal uit een gestolen kluis. Toch kan de beveiliging van persoonsgegevens tekortschieten. Dit kan gebeuren als bestanden niet afdoende beveiligd zijn, of als menselijke fouten worden gemaakt. Zelfs als dit onbewust of ongewild gebeurt, denk aan het verkeerd adresseren van post of een mail, wordt gesproken over een inbreuk op de beveiliging (van de persoonsgegevens).
Wanneer een datalek plaatsvindt bij een verwerker van persoonsgegevens (een IT leverancier) moet de gemeente als verantwoordelijke te allen tijde zelf als verantwoordelijke afwegen of er melding moet worden gemaakt aan de AP of aan de betrokkene(-n). Immers, de gemeente blijft eigenaar van de gegevens.

Om de verantwoordelijkheid van de beveiliging goed af te bakenen, is de juiste toepassing van de verwerkersovereenkomst zoals genoemd in hoofdstuk 5 paragraaf 5.3.2 essentieel. Naast de verplichtingen omtrent het melden aan de AP en eventueel betrokkene(-n), kunnen de volgende praktische stappen genomen worden door de privacybeheerder, informatiebeveiligingsbeheerder, FG, CISO, directeur/afdelingshoofd;

- Het inschakelen van de juridische afdeling;
- Duidelijke situatieschets van constatering, vervolgacties en verantwoordelijkheden;
- Veiligstellen van data en bewijs, waaronder logboeken en back-ups;
- Een schrijven naar de betrokkene en/of persbericht/ bericht voor meerdere betrokkenen opstellen.

6 Planning- en control cyclus

Om de privacy van haar inwoners blijvend te borgen binnen de gemeentelijke organisatie, wordt gebruikt gemaakt van een planning- en control cyclus. Dit gebeurt binnen de gemeente aan de hand van een plan-do-check-act cyclus zoals weergegeven in figuur 2.

De FG houdt toezicht op de planning- en control cyclus en stuurt deze aan waar nodig. Jaarlijks wordt de aan de hand van de planning- en control cyclus rapportage uitgebracht aan het college als hoogste organisatorische orgaan. Een korte toelichting op de verschillende fasen is in dit hoofdstuk uitgewerkt.
Figuur 3: Plan-do-check-act cyclus
6.1 Plan
De planningsfase bestaat uit de strategische en tactische werkzaamheden rondom de bescherming van persoonsgegevens. Het privacy beleidskader omvat alle wettelijke richtlijnen en ambities van de organisatie om privacybescherming in te bedden binnen alle processen waarop ze van toepassing is. Door dit beleid is het voor elke werknemer duidelijk wat het standpunt van de gemeente is en wat de standaard is waaraan de werkprocessen dienen te voldoen.
Met het privacy beleidskader als stip op de horizon, is de volgende stap het bepalen van de huidige situatie. Hierbij worden werkprocessen geïnventariseerd, de documentatie van gegevens onder de loep

genomen etc. Door in kaart te brengen waar de gemeentelijke organisatie op dat moment staat, kan er een inventarisatie gemaakt worden van de zaken die niet overeenkomstig zijn met het privacy beleidskader. Zo kan doelgericht actie ondernomen worden tot verbetering.

De zaken die verbetering behoeven kunnen concreet beschreven worden aan de hand van de huidige en gewenste situatie, waardoor het raamwerk voor een strategie ontstaat. Om de strategie gestalte te geven en tastbaar te maken, kan in elk geval rekening gehouden worden met drie stappen die ondernomen worden in een veranderproces: Ontwerpen, acceptatie en implementatie. Door deze zaken op een rij te krijgen, kan er efficiënt actie ondernomen worden bij de volgende fase.

6.2 Do

Als de strategie is opgesteld, kan er actie ondernomen worden. Aangezien privacybescherming een doorlopend thema is binnen verschillende werkprocessen zal de focus van de strategie voornamelijk liggen, maar is niet beperkt tot, de inrichting hiervan. Door de processen vorm te geven naar de laatste standaard die opgenomen is in het beleid, kan de inwoner vertrouwen dat de gemeente zorgvuldig met hun gegevens omgaat.

Buiten deze processen op papier, is het zaak dat bij de menselijke handelingen in deze zorgvuldig omgegaan wordt bij het verwerken van persoonsgegevens. Het belang hiervan wordt later beschreven in het hoofdstuk 'Cultuur en Bewustwording'. Om medewerkers te blijven herinneren aan het belang van de zorgvuldige omgang met gegevens, dient het bewustzijn hiervan periodiek gestimuleerd te worden.

6.3 Check

In deze fase van de planning- en control cyclus wordt gecontroleerd of de plannen die er waren en uitgevoerd zijn, naar behoren werken. Om dit in te delen wordt er onderscheid gemaakt tussen monitoring en handhaving van het beleid. De monitoring richt zich op de interne processen en bewustwording, de handhaving wordt (deels) opgelegd door externe partijen/derden.

6.3.1 Monitoring

De controle van de processen en bewustwording is een essentieel onderdeel van de cyclus en wordt uitgevoerd door de FG, die daar de wettelijke bevoegdheden toe heeft. Na de uitgevoerde controles wordt er een rapportage/evaluatie opgesteld, waaruit blijkt of het beleid voldoende is geborgd, of dat er meer sturing nodig is. De controlemiddelen kunnen zijn, maar zijn niet beperkt tot:

- Interne audit op werkprocessen
- Feedbackgesprekken met uitvoerende werknemers
- Feedbackgesprekken met burgers
- Interne steekproeven
- Privacy Impact Analyse

Van belang is in deze fase dat er uitgegaan wordt van een werkbare situatie voor de gemeente, waarbij de gegevens van de inwoners voldoende geborgd zijn.

6.3.2 Auditlast privacy

Elk jaar moet de gemeente zich verantwoorden over de kwaliteit van informatieveiligheid en privacy binnen de verschillende werkvelden. Met betrekking tot informatiebeveiliging gebeurde dit tot 2017 middels verschillende zelfevaluaties voor onder andere de Basisregistratie Personen (BRP), Digitale persoonsidentificatie (DigiD) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet). Omdat deze auditlast versnipperd over het gehele jaar plaatsvond, werd besloten om vanaf 2017 een nieuwe audit systematiek in te voeren. Met de Eenduidige Normatiek Single Information Audit (ENSIA) werd het beantwoorden van de uitvraag betreft informatieveiligheid gecombineerd tot één zelfevaluatie.

Inzake de verantwoording over de kwaliteit van privacy ontbreekt tot op heden helaas nog steeds een dergelijke eenduidige audit-systematiek. De FG rapporteert echter binnen de planning & control cyclus, aan de hand van een bijdrage in de bedrijfsvoeringsrapportage, en middels een FG-jaarverslag, over de uitvoering van privacy beleidskader, de stand van zaken met betrekking met betrekking gerealiseerde privacy maatregelen en datalekken. De FG voert op basis de AVG desgevraagd of op eigen initiatief een audit(s) uit op de uitvoering van (bepaalde delen) van het privacy beleidskader van de gemeente. De FG koppelt zijn bevinden aan de hand van een auditrapport terug aan de ·(eind-)verantwoordelijke.

6.3.3 Handhaving

Door de aanstelling van de AP bestaat er in Nederland een actief orgaan om de naleving van de wetgeving omtrent persoonsgegevens te controleren. De AP heeft taken en bevoegdheden om de handhaving van de AVG na te leven. Zo heeft de AP de bevoegdheid om onderzoek te doen naar gegevensverwerking binnen de gemeente en heeft zij de functie van waakhond waar burgers misstanden kunnen melden. Bij vermeende misstanden kan er een onderzoek door de AP worden ingesteld, maar kan er ook gebruik gemaakt worden van zogeheten 'alternatieve interventies'. Dit zijn waarschuwingen in de vorm van een brief of gesprek, waarin de vermeende misstanden aangekaart worden. De AP heeft bij misstanden de bevoegdheid om rechtsvordering in te stellen. Zo kan de AP besluiten tot het stopzetten

van verwerking van persoonsgegevens en bestuurlijke boetes opleggen. De risico's voor het niet naleven van de AVG kunnen worden nageslagen in het hoofdstuk 7.

6.4 Act
De laatste stap in de planning & control cyclus is het handelen naar aanleiding van de evaluatie die voortvloeit uit de monitoring of handhaving. De actiepunten die worden geconstateerd worden in deze fase uitgevoerd om te voldoen aan het gestelde beleid. Verder hoort in deze fase de incidentmeldingen omtrent privacy thuis. Deze meldingen zijn veelal ad hoc, waarvoor door de werkgroep informatieveiligheid de juiste expertise in huis heeft. Zij zullen de juiste beoordeling aan de incidenten geven en hier de nodige stappen voor ondernemen. Als de cyclus beëindigd is, wordt een jaarlijkse rapportage verzorgd aan het college over de ontwikkelingen tijdens de planning & control cyclus. Na deze rapportage wordt weer aangevangen met de cyclus en worden het beleid en de strategie herzien.

7 Risico's

Bij het omgaan met persoonsgegevens kunnen ook enkele organisatorische risico's onderscheiden worden, die daarmee op zowel korte als lange termijn gevolgen hebben. Door deze risico's in kaart te hebben, kunnen gerichte maatregelen genomen worden in de privacy strategie om deze risico's zo veel als mogelijk te voorkomen. De grootste oorzaken, risico's en gevolgen zijn opgenomen in de risicoboom in bijlage 11.
De grootste risico's voor het welslagen van het privacybeleid met de daaraan herleidde gevolgen zijn (zie bijlage 11) :
- Het niet accepteren van verantwoordelijkheid
Door het niet naleven van het privacybeleid van de gemeente bestaat het risico dat de verantwoordelijkheid over de persoonsgegevens niet genomen wordt.

- Het niet naleven van de planning- en control cyclus
Door weinig bewustwording in de naleving van het privacybeleid bestaat de kans dat de organisatie zich niet committeert aan de cyclische bedrijfsvoering omtrent privacy.

Mochten deze risico's werkelijkheid worden, dan kan er geen correcte informatievoorziening aan het college plaatsvinden. Als dit structureel nagelaten wordt, bestaat de kans op een vertrouwensbreuk tussen de inwoners en de gemeente. Dit kan voorkomen worden door nadruk te leggen op de bewustwording in de naleving van het privacybeleid.

- Het niet legitiem verwerken van persoonsgegevens
Door het niet sturen op bewustwording in het naleven van de privacywetgeving en het daarop geijkte beleid, bestaat het risico dat gegevens niet legitiem verwerkt worden.

- Niet informeren van de betrokkenen
Door het niet sturen op bewustwording in het naleven van de privacywetgeving en het daarop geijkte beleid, bestaat het risico dat de betrokkenen niet of onjuist geïnformeerd worden over de verwerking van hun gegevens.
Bovenstaand risico betreffende de legitimiteit van verwerking kan leiden tot sociale beschadiging. Wanneer de inwoners van de gemeente dit treft, kan dit een zekere mate van ongemak opleveren. Dit kan uiteindelijk leiden tot imagoschade of een vertrouwensbreuk tussen inwoners en gemeente. Verder kunnen beide risico's leiden tot een onvrijwillig onderzoek van de AP, die bij het vaststellen van misstanden bevoegd is om per incident een bestuurlijke boete op te leggen. Deze boetes kunnen oplopen tot €810.000 per overtreding, exclusief eventuele schadevergoeding voor getroffen burgers.
- Geautomatiseerde besluitvorming - profilering
Wanneer de gemeente besluit over te gaan op het profileren van haar burgers, bestaat het risico dat er geautomatiseerde beslissingen over natuurlijke personen genomen worden.
Dit risico kan als gevolg hebben dat de persoonlijke veiligheid van de inwoners van de gemeente in het gedrang komt en deze sociale schade oplopen door bijvoorbeeld stigmatisering of dat iemand 'gevangen' zit in een (verkeerd of niet-actueel) profiel, omdat de menselijke tussenkomst ontbreekt. Dit levert ongemak voor de betrokkene op, wat kan leiden tot imagoschade of een vertrouwensbreuk tussen inwoners en de gemeente. Verder kunnen signalen van geautomatiseerde besluitvorming leiden tot een bovengenoemd onderzoek door de AP.
Om risico's te beheersen zal in de privacy strategie jaarlijks bepaald moeten worden welke maatregelen genomen worden om de risico's te beperken. Deze kunnen enerzijds gericht zijn op de oorzaak door preventief in te zetten op de bescherming van de privacy van de inwoners van de gemeente. Anderzijds kunnen maatregelen getroffen worden op basis van de gevolgen door eventueel extra capaciteit in te bouwen 'voor het geval dat'.
Meer risico's komen aan bod door het periodiek uitvoeren van een Gemeentebrede GAP-analyse. Om te blijven sturen op de bescherming van privacy wordt een analyse gemaakt bij de 'check'-fase van de planning- en control cyclus.

Aldus vastgesteld door het college van burgemeester en wethouders van de gemeente Kerkrade in zijn vergadering van 22 januari 2019,
Het college, de secretaris,
J.J.M. Som H.J.M. Coumans MPM

Voetnoten

1. Onder persoonsgegevens wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
2. Onder het verwerken van persoonsgegevens wordt verstaan: het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigingen van persoonsgegevens.
3. Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
4. Naam, Adres en Woonplaats.
5. Verwerken van persoonsgegevens: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigen.
6. Art. 37 AVG
7. Art. 5 lid 1 sub a en art. 6 AVG
8. Art. 24 AVG
9. Art. 17 AVG
10. Art. 15 lid 3 AVG
11. Art. 22 AVG
12. Art. 6 lid 4 sub e AVG
13. Artikel 3 lid 1 juncto artikel 4 lid 7 AVG. In de meeste gevallen wordt het college als verwerkingsverantwoordelijke aangemerkt, echter in sommige specifieke gevallen kan dit ook de burgemeester of een derde/samenwerkingspartner zijn.
14. Artikel 35 AVG. Een GegevensEffectBeoordeling (PIA) maakt onderdeel uit van het procesplan.
15. Artikel 35 lid 11 AVG.
16. Artikel 5 lid 1 sub b AVG.
17. Artikel 5 lid 1 sub c AVG.
18. Overweging 79 juncto artikel 32 AVG.
19. Overweging 59 AVG juncto artikel 12 lid 4 AVG.
20. Artikel 35 lid 1 juncto lid 11 AVG.
21. Overweging 39 juncto artikel 39 lid 1 sub b AVG.
22. Overweging 5 tot en met 88 juncto artikel 32, 33 en 34 AVG.
23. Vergelijkbaar met de evaluatie en actualisering van het informatiebeveiligingsbeleid.
24. Vergelijkbaar met het informeren van de raad op het gebied van de informatiebeveiligingsbeleidsuitvoering (ENSIA-systematiek)
25. Overweging 97 juncto artikel 37 AVG.
26. Archivering is ook van belang (bewaren en vernietigen van persoonsgegevens).
27. Deze derden zijn onder de AVG zelf ook verwerkingsverantwoordelijke (artikel 4 lid 7 AVG), maar dan alleen voor hun eigen persoonsgegevensverwerkingen.
28.https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf
29. Overweging 74 en 78 AVG en juncto artikel 5 AVG.
30. Vergelijk met horizontale verantwoording richting gemeenteraad met betrekking tot de ENSIA.
31. Artikel 74en 78 AVG juncto artikel 24 lid 1 AVG.
32. Overweging 82 AVG juncto artikel 30 AVG.
33. Overweging 97 AVG juncto artikel 37 lid 1 sub a AVG.
34. Op basis van artikel 38 lid 3 AVG rapporteert de FG rechtstreeks aan de hoogste leidinggevende van de verwerkingsverantwoordelijke.
35. VNG Handreiking: “Rol en taken van de FG”
36. Artikel 39 lid e AVG.
37. Artikel 38 lid 3 AVG.
38. Overwegingen 81, 82, 83, 85, 90, 91 AVG juncto Artikel 28, 30 , 33, 35, 38 en 39 AVG.
39. Art. 4 lid 1 AVG
40. Art. 9 lid 1 AVG
41. Genetische gegevens waarmee het mogelijk is om de identiteit van een persoon vast te stellen, zoals DNA.
42. Biologische gegevens waarmee het mogelijk is om de identiteit van een persoon vast te stellen. Daarvoor worden unieke onderdelen van het lichaam gebruikt zoals een vingerafdruk.
43. Art. 9 AVG
44. Art. 5 lid b AVG
45. Artikel 6 lid 1 AVG.
46.https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapport_de_rol_van_toestemming_in_het_sociaal_domein.pdf

47. Met sociaal domein wordt bedoeld de uitvoering van taken op het gebied van de Jeugdwet, de Wmo 2015, de Participatiewet, de Wet gemeentelijke schuldhulpverlening en de Wet passend onderwijs.
48. Art. 12 AVG
49. Art. 13 AVG
50. Art. 28 AVG

51. Art. 32 AVG
52. Art. 28 lid 3 sub h AVG
53. Overweging 60, 61 en 62 AVG juncto artikel 13 en 14 AVG.
54. Overweging 59 AVG juncto artikel 12 lid 4 AVG
55. Overweging 63 AVG juncto artikel 15 AVG.
56. Overweging 65 AVG juncto artikel 16 AVG.
57. Overweging 65 en 66 AVG juncto artikel 17 AVG.
58. Artikel 18 AVG.
59. Overweging 68 juncto artikel 20 AVG.
60. Overweging 69 juncto artikel 21 AVG.
61. Overweging 70 en 71 juncto artikel 22 AVG.
62. Overweging 91 AVG artikel 35 AVG.
63. Artikel 5 lid 1 onder f juncto artikel 32 AVG
64. Artikel 33 AVG.
65. Artikel 34 AVG.
66. Artikel 34 lid 2 AVG
67. Artikel 34 lid 2 juncto Artikel 33 lid 3 sub b AVG
68. Artikel 34 lid 2 juncto Artikel 33 lid 3 sub c AVG
69. Artikel 34 lid 2 juncto Artikel 33 lid 3 sub d AVG