Privacybeleid

Rekenkamercommissie Dordrecht

11 DECEMBER 2018

In opdracht van	Rekenkamercommissie Dordrecht
Status	*Concept*
Versie	0.1
Redacteur	Paula van der Knaap
Datum	01-12-2018

Versiebeheer			
Versie	***Datum***	***Wijzigingen***	***Auteur***
0.1	01-12-2018	Initiële versie.	Paula van der Knaap

Goedkeuring				
Versie	***Datum***	***Naam***	***Functie***	***Status***
0.1	11-12-2018	Drs. K. Meijer	Plv. Voorzitter RKC Dordrecht	
0.1	11-12-2018	Drs. C. E. J. M. Cransveld	Lid RKC Dordrecht	
0.1	11-12-2018	Mr. Drs. F.M. Lagerveld	Secretaris RKC Dordrecht	

Distributielijst		
Versie	***Datum***	***Naam***
0.1	03-12-2018	Mr. Drs. F.M. Lagerveld

Tekenparagraaf

Organisatie	**Naam**	**Handtekening**	**Datum**
Rekenkamercommissie	Drs. K. Meijer		18-12-18

Inhoud

1. Inleiding

1.1 Aanleiding

Gemeenten en gemeentelijke organisaties verwerken persoonsgegevens om een dienst te verlenen, een product te leveren of om andere doelen te bereiken. Het belang van de gemeenten en gemeentelijke organisaties om persoonsgegevens te verwerken kan op gespannen voet staan met het privacybelang van de betrokkene op wie de verzamelde gegevens betrekking hebben.

Het beschermen van privacybelangen wordt vaak gezien als obstakel bij het uitvoeren van de werkzaamheden, omdat moet worden getoetst of aan de privacywetgeving wordt voldaan. Maar privacy is een belangrijk grondrecht. In de Grondwet is verankerd dat de overheid niet zomaar persoonlijke gegevens mag gebruiken.
Het is een wettelijke verplichting dat overheidsorganisaties behoorlijk en zorgvuldig omgaan met persoonsgegevens in verband met de privacy van betrokkenen.

De regio Drechtsteden heeft privacy beleid geformuleerd, waarin beschreven staat hoe om te gaan met de verwerking van persoonsgegevens. Binnen de gemeente Dordrecht is dit privacybeleid van toepassing.
De Rekenkamercommissie Dordrecht (hierna te benoemen als RKC) conformeert zich derhalve aan het geformuleerde privacybeleid van de gemeente Dordrecht.

In het privacybeleid staan kaders beschreven voor het verwerken van privacygevoelige informatie of te wel persoonsgegevens, de bescherming van deze gegevens en omgang met deze gegevens. Dit beleid dient als kapstok, waarbij voor een specifiek vakgebied een beheerplan of privacy-protocol dient te worden opgesteld.

De werkzaamheden van de RKC betreffen onderzoeken naar de doelmatigheid, doeltreffendheid en rechtmatigheid van het door het gemeentebestuur gevoerde bestuur. Hiervoor verwerkt de RKC soms persoonsgegevens (bijvoorbeeld NAW- of uitkeringsgegevens) en soms bijzondere persoonsgegevens (bijvoorbeeld medische gegevens). Voorafgaand aan elk onderzoek weegt de RKC zorgvuldig af welke gegevens nodig zijn voor het onderzoek, zodat dit met zo min mogelijk gegevens kan worden uitgevoerd.

Het privacybeleid sluit aan bij het Informatiebeveiligingsbeleid Drechtsteden. Immers, informatiebeveiliging en het veilig en verantwoord werken met persoonsgegevens overlappen elkaar voor een groot deel. Voor het borgen van de bescherming van persoonsgegevens is het naleven van wat is geregeld in het Informatiebeveiligingsbeleid Drechtsteden dan ook van cruciaal belang.

De Autoriteit Persoonsgegevens (verder te noemen AP) is de externe toezichthouder op een behoorlijke en zorgvuldige verwerking van persoonsgegevens binnen Nederlandse organisaties, waaronder overheden. Er kan vanaf 25 mei 2018 een boete worden opgelegd door de AP die een substantieel en afschrikwekkend karakter zal hebben, indien zij een overtreding constateert (maximaal 20 miljoen euro).

2 Uitgangspunten

2.1 Doelstellingen van het beleid

Doelstelling van het beleid is dat binnen de RKC op een verantwoordelijke wijze en binnen wettelijke kaders met privacy gevoelige gegevens wordt omgegaan. Binnen de wettelijke kaders probeert de RKC creatieve oplossingen te vinden om de regulieren werkprocessen en innovaties goed uit te kunnen voeren.
Het wettelijk kader voor bescherming van persoonsgegevens wordt, naast vele specifieke wetten, aangegeven door de AVG. De eisen die de AVG stelt aan het verwerken van persoonsgegevens zijn dan ook zorgvuldig geïmplementeerd bij de RKC. Als startpunt is het verplichte bewustwordingsprogramma voor alle medewerkers opgezet. De privacybescherming kan zo stapsgewijs worden verhoogd en vormt de basis voor de vergroting van het privacy-bewustzijn en de verdere professionalisering binnen de RKC.

De RKC wilt onder andere hiermee bereiken dat:

- de basis voor een goed geïmplementeerd privacybeleid wordt gegarandeerd en dat alle interne medewerkers en ingehuurde onderzoekers en externen zich ten volle bewust zijn van de noodzakelijkheid van een zorgvuldige omgang met persoonsgegevens. Dit vormt de basis voor een toepassing van de wettelijke eisen en voor een respectvolle omgang met de persoonsgegevens van betrokkenen;
- de rechten van betrokkenen worden gerespecteerd en in onze procedures zijn verankerd;
- het vertrouwen van betrokkenen in de overheid niet wordt beschaamd;
- uitvoering van het privacybeleid binnen de RKC gericht wordt opgepakt, zodat de wettelijke eisen goed geïmplementeerd zijn;
- het onderwerp breed wordt gedragen binnen alle bestuurlijke en ambtelijke lagen van de RKC, als onderdeel van zowel uitvoering van de wettelijke opgave, goed werkgeverschap, opdrachtgeverschap en opdrachtgeverschap;
- de kans op financiële schade door het oplopen van boetes en reputatieschade wordt geminimaliseerd.

2.2 Begrippenkader

Begrippen die voor een goede uitvoering van het privacybeleid van groot belang zijn en worden gehanteerd binnen de AVG zijn:

Begrip	**Omschrijving**
Accountability	Het kunnen aantonen op welke manier de persoonsgegevens worden verwerkt conform de AVG. Hiertoe dienen passende en effectieve maatregelen te worden genomen, zoals: • documentatie plicht: het bijhouden van een Register van verwerkingen; • het beschermen van gegevens door ontwerp principes als Privacy by Design en Privacy by Default; • indien van toepassing het uitvoeren van een Privacy Impact Assessment, PIA; • het treffen van passende technische - en organisatorische maatregelen, waaronder juridische - en beveiligingsmaatregelen; • het opstellen van een procedure om beveiligingsincidenten en datalekken te documenteren. Vervolgens een procedure voor het melden van een datalek aan AP; • het aanstellen van een Functionaris Gegevensbescherming.

Algemeen Bestuur (AB) Drechtsteden	Elk algemeen bestuur van elke gemeenschappelijke regeling, inclusief de Drechtraad.
Algemeen Bestuur (AB) RKC	Voorzitter en commissieleden RKC
Dagelijks Bestuur (DB) Drechtsteden	Elk dagelijks bestuur van elke gemeenschappelijke regeling, inclusief het Drechtstedenbestuur.
Dagelijks Bestuur (DB) RKC	Secretariaat RKC
Betrokkene	De natuurlijke persoon van wie de gegevens worden verwerkt.
Functionaris Gegevens-bescherming (FG)	De FG is de interne toezichthouder op de verwerking van persoonsgegevens. De FG dient in alle onafhankelijkheid zijn werkzaamheden te kunnen uitvoeren en ontvangt daarbij geen instructies van opdrachtgevers of verwerkers. Hij is aangemeld bij de AP als contactpersoon en aanspreekpunt voor de meldingen van datalekken. Hij functioneert als tussenpersoon tussen verschillende belanghebbenden en is daarmee ook verlengstuk van de Autoriteit Persoonsgegevens (AP).
Gegevensbeschermings-effectbeoordeling, ofwel Privacy Impact Assessment (PIA):	Methode om de effecten en risico's van nieuwe of bestaande verwerkingen op de bescherming van de privacy te beoordelen.
Governance	De wijze waarop de daadwerkelijke implementatie van richtlijnen en strategie is gegarandeerd, zodat vereiste processen op de juiste manier worden gevolgd om te kunnen voldoen aan wet- en regelgeving. Governance bevat het definiëren van rollen en verantwoordelijkheden, meten en rapporteren, nemen van acties om geïdentificeerde kwesties op te lossen.
Inbreuk in verband met persoonsgegevens, ofwel Datalek	Een inbreuk op de beveiliging die al dan niet per ongeluk op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene) als bedoeld in de AVG of daarvoor in de plaats tredende wetgeving. Naast gewone persoonsgegevens, zoals naam en adresgegevens, kent de wet ook bijzondere persoonsgegevens, zoals etnische achtergrond, politieke voorkeur of gezondheid.
Privacybescherming	Het omgaan met persoonsgegevens conform de eisen in de AVG.
Privacy-coördinatoren	Medewerkers van het Secretariaat RKC. Zij zijn het interne aanspreekpunt voor de organisaties en communiceren en rapporteren aan/met de FG.
Proceseigenaren	Degenen die binnen de organisatie zijn aangewezen als verantwoordelijke voor een proces.
Verwerking	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken

	door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
Verwerkings-verantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst die of een ander orgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

2.3 Juridisch kader – basiseisen uit de AVG

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkenen voorop. Er moet worden voorkomen dat er onnodige of te verregaande inbreuken worden gemaakt. De AVG regelt het algemene kader voor de omgang met persoonsgegevens binnen de landen van de Europese unie.

De AVG is de hoogste wetgeving voor privacybescherming en fungeert als een parapluwet die van toepassing is voor alle verwerkingen van persoonsgegevens door organisaties, zowel bedrijven als overheden. De uitgangspunten van de AVG zijn:

- Verwerking op rechtmatige, behoorlijke en transparante wijze (artikel 5a AVG);
- Verzamelen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 5b AVG);
- Alleen verwerking op één van de in de AVG opgenomen grondslagen (artikel 6 AVG).

Van belang is dat persoonsgegevens worden verwerkt voor een duidelijk omschreven doel, de doelbinding. Hieruit kan de grondslag voor verwerking vastgesteld worden. De grondslagen zijn limitatief opgesomd in artikel 6 AVG. Vervolgens moet worden vastgesteld dat de verwerkte persoonsgegevens proportioneel zijn (worden er niet meer gegevens verwerkt dan noodzakelijk voor het uitoefenen van de taak) en dat aan het subsidiariteitsbeginsel wordt voldaan (is er een voor de betrokkene minder belastende manier om de taak uit te voeren).

Bijzondere categorieën van persoonsgegevens zijn persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid blijkt (artikel 9 AVG). Financiële gegevens en het BSN zijn gevoelige persoonsgegevens. Het verwerken van bijzondere en gevoelige persoonsgegevens (artikel 9 AVG) en het verder verwerken van reeds verzamelde gegevens (artikel 6.4 AVG), is zelfs aan zeer strikte voorwaarden gebonden.

De betrokkene kan altijd inzage of wijziging van de verwerkte persoonsgegevens opvragen.
Om het proces van gegevensverwerking ordelijk te laten verlopen en betrokkenen (burgers) makkelijk toegang te geven tot de RKC, stelt de RKC een Functionaris Gegevensbescherming (FG) aan.

De RKC heeft de wettelijk verplichting om gegevensbescherming te borgen. Dit moeten zij doen door technische en organisatorische maatregelen te treffen[1]. Informatieveiligheid is hier een groot onderdeel van. Samen met onder andere informatiebeheer, het juridisch

[1] Zie Artikel 15 AVG.

kader en privacy-bewustzijn zorgt informatieveiligheid voor de borging van bescherming van privacygevoelige gegevens. Voor de informatieveiligheid maakt de RKC gebruik van de diensten op ICT gebied binnen de Drechtsteden. Er wordt gewerkt binnen de kaders van het Informatiebeveiligingsplan en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
Het privacybeleid van de RKC gaat uit van het voldoen aan de eisen van de AVG en de Uitvoeringswet AVG. Daarnaast zijn er diverse specifieke wetten, zoals de BRP, WMO, Jeugdwet, Politiewet, die aanvullende eisen stellen aan privacybescherming. Deze wetten worden in dit beleidsstuk niet ingevuld.

2.4 Wijze van inrichten gegevensverwerking

Door het cyclische karakter van de aangegeven maatregelen en door privacy vast op de agenda's van de RKC te geplaatsen, ontstaat een continue proces van veranderen en verbeteren. De kwaliteit van het omgaan met privacyvraagstukken wordt verhoogd door op verschillende niveaus en vanuit verschillende rollen telkens weer de PDCA[2]-cyclus te doorlopen. Hierdoor ontstaat een evenwichtig privacy-beheersingssysteem.
Medewerkers van de RKC dienen privacy als onderdeel van hun werk- overleggen op te nemen. Het borgen van de privacy is onlosmakelijk verbonden met informatiebeveiliging. Om afdelingen te ondersteunen zullen experts ingezet worden op het gebied van gegevensverwerking en informatiebeveiliging. Deze experts werken nauw met elkaar samen.

2.5 Doelgroep

Het privacybeleid voor de RKC is van toepassing op alle taken en processen waar de RKC voor verantwoordelijk is. Dit privacybeleid en een juiste uitvoering hiervan richt zich tot *alle* interne en externe medewerkers[3] binnen de RKC. Het is vooral gericht op diegenen die werken met persoonsgegevens, dan wel persoonsgegevens laten verwerken door externe partners. De voorzitter, leden en het secretariaat spelen een belangrijke rol bij de besluitvorming over dit onderwerp en de sturing ervan in de planning- & control cyclus.

2.6 Ingangsdatum

De AVG is per 25 mei 2018 van kracht en zal per die datum worden gehandhaafd door de AP. De Nederlandse Wet Bescherming Persoonsgegevens (Wbp) en de Europese Richtlijn 95/46, waarop de Wbp is gebaseerd, komen per gelijke datum te vervallen.

[2] De Cirkel van Deming: Plan-Do-Check-Act. Continue verbeter cirkel.
[3] In dit verband is een *medewerker* iemand die werkzaam is bij of werkzaamheden verricht voor / in opdracht van de RKC.

3 Rechten van betrokkenen

Binnen de AVG krijgen betrokkenen nieuwe privacy rechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt, meer dan onder de Wbp, op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden (accountability).

De rechten van de betrokkene moeten binnen de organisaties op transparante wijze zijn ingericht. Betrokkenen hebben recht op:

- op inzage van gegevens (artikel 15 AVG);
- op rectificatie van gegevens (artikel 16 AVG);
- op gegevenswissing, recht op "vergetelheid" (artikel 17 AVG);
- beperking van de verwerking (artikel 18 AVG);
- kennisgevingplicht inzake rectificatie, wissing of beperking (artikel 19 AVG);
- op overdraagbaarheid van gegevens, dataportabiliteit (artikel 20 AVG).

3.1 Recht op inzage van gegevens (artikel 15 AVG)

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke uitsluitsel te krijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens.

De betrokkene heeft het recht om te informeren of zijn persoonsgegevens worden verwerkt. Als dat het geval blijkt, heeft hij recht op uitleg over het wat en het hoe, als ook op inzage en een kopie van zijn persoonsgegevens (zie nader artikel 20 AVG). De verwerkingsverantwoordelijke kan verlangen dat de betrokkene zich op adequate wijze identificeert. Het recht van inzage is mede bedoeld om uitoefening van de rechten van een rectificatie (artikel 16 AVG) gegevenswissing (artikel 17 AVG) of beperking (artikel 18 AVG) mogelijk te maken.

3.2 Recht op rectificatie van gegevens (artikel 16 AVG)

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld een rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen, met in achtneming van de doeleinden van de verwerking.

Wanneer verwerkte persoonsgegevens onjuist of onvolledig zijn, heeft de betrokkene het recht deze te laten corrigeren of aanvullen. Dit artikel is een uitwerking van artikel 5, lid 1, sub d, het beginsel van juistheid van persoonsgegevens.
De verwerkingsverantwoordelijke en de verwerker moeten alle redelijke maatregelen nemen om er voor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd. Het is daarbij irrelevant of de onjuistheden berusten op een fout van verwerkings-verantwoordelijke of verwerker.

3.3 Recht op gegevenswissing, recht op "vergetelheid" (artikel 17 AVG)

De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging, wissing van hem betreffende persoonsgegevens te verkrijgen. De verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer dit van toepassing is.

Op grond van de beginselen van juistheid (artikel 5 AVG) en opslagbeperking (artikel 5 AVG) mogen persoonsgegevens niet langer worden bewaard dan nodig is voor het doel van hun verwerking. Het recht van gegevenswissing werkt dit nader uit tot een recht

voor de betrokkene om overtollige persoonsgegevens gewist te krijgen met corresponderende plicht voor de verwerkingsverantwoordelijke (en uiteraard zijn verwerkers).

3.4 Recht op beperking van de verwerking (artikel 18 AVG)

De betrokkene heeft het recht van de verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen.

Beperking is enigszins circulair gedefinieerd (artikel 4 AVG) als het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken. Kort gezegd komt het erop neer dat men een tijdelijk slot op de verwerking van persoonsgegevens wil totdat een bezwaar of een probleem is opgelost.

3.5 Kennisgevingsplicht inzake rectificatie, wissing of beperking (artikel 19 AVG)

De verwerkingsverantwoordelijke stelt iedere ontvanger (niet zijnde betrokkene) aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie of wissing van betreffende persoonsgegevens of beperking van de verwerking overeenkomstig artikel 16 AVG, artikel 17 AVG en artikel 18 AVG, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De verwerkings-verantwoordelijke verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

Wanneer de verwerkingsverantwoordelijke een rectificatie (artikel16 AVG) gegevenswissing (artikel 17 AVG) of beperking (artikel 18 AVG) van persoonsgegevens van betrokkene uitvoert, is hij verplicht alle ontvangers van die persoonsgegevens hierover in te lichten. Doel van deze kennisgeving is dat deze ontvangers de betreffende rectificatie, wissing of betrekking ook doorvoeren.

3.6 Recht op overdraagbaarheid gegevens, dataportabiliteit (artikel 20 AVG)

Naast het al langer bekende recht van inzage in persoonsgegevens (artikel 15 AVG) introduceert de AVG een nieuw recht namelijk dataportabiliteit, oftewel overdraagbaarheid van persoonsgegevens.

De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machinaal leesbare vorm te verkrijgen en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt.

4 Werkprocessen

4.1 Omgaan met persoonsgegevens

Persoonsgegevens worden alleen verwerkt voor het uitvoeren van bepaalde wettelijke taken en vastgestelde regelingen. Zie ook paragraaf 2.3 Juridisch kader. In het merendeel van de gevallen worden persoonsgegevens door de betrokkene zelf verstrekt. Veel gebruikte gegevens of al bekende gegevens die zijn opgenomen in basisregistraties of andere authentieke bronnen, worden daaruit opgevraagd. Dit is in overeenstemming met het principe van 'eenmalige uitvraag en meervoudig gebruik' dat door de overheid en de gemeente wordt gepropageerd.

De RKC verwerkt voor haar onderzoeken soms ook persoonsgegevens die bij de gemeente of bijvoorbeeld een gesubsidieerde instelling worden opgevraagd. Zij zijn op grond van de gemeentewet verplicht deze gegevens aan de RKC te verstrekken en u daarover te informeren. Deze gegevens laat de RKC verwerken zonder u daarover nog afzonderlijk te informeren. De analyse van deze gegevens worden door de RKC gebruikt in de rapporten van de RKC. De gebruikte persoonsgegevens worden niet openbaar gemaakt of met anderen gedeeld.
Ook komt het voor dat de RKC u om persoonsgegevens vraagt, bijvoorbeeld via een enquête, een interview of een groepsgesprek. Sporadisch kan het voorkomen dat de RKC u om bijzondere persoonsgegevens zal vragen (zoals medische gegevens) als de RKC bijvoorbeeld een onderzoek (laat) doen in het sociaal domein. Ook kan het voorkomen dat de RKC u toestemming zal vragen om een (deel) van uw gemeentelijk dossier, waarin bijzondere persoonsgegevens staan, te mogen onderzoeken. De (bijzondere) persoonsgegevens worden pas door de RKC verzameld als u daarmee expliciet akkoord bent gegaan. Ook voor deze persoonsgegevens geldt dat de RKC deze niet openbaar maken.
Alleen met uw uitdrukkelijke toestemming nemen wij uw naam en functie op in ons rapport.

Van politici die verbonden zijn aan de gemeente Dordrecht registeren de RKC naast contactgegevens één bijzonder persoonsgegeven: de politieke partij waar zij lid van zijn. Bij het benaderen van raadsleden voor het onderzoeksprogramma of de onderzoeken van de RKC nemen wij een zo groot mogelijke spreiding van politieke overtuiging in acht.

Meestal worden gegevens in informatiesystemen opgenomen waar ze alleen toegankelijk zijn voor de medewerkers die belast zijn met het uitvoeren van de taak.
Informatiesystemen moeten voldoen aan de eisen van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

4.2 Bewustwording.

Zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede Informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak van bewustwording en communicatie. Beleid en maatregelen zijn niet voldoende om risico’s op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico’s wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.
De bedrijfscultuur in zijn geheel moet op een "bewust bekwaam" niveau van omgaan met persoonsgegevens worden gebracht. Er moet een constante afweging worden gemaakt tussen "need to know" en "nice to know", waarbij in de laatste categorie geen persoons-gegevens worden verwerkt.

Het is van groot belang dat medewerkers die daadwerkelijk werken met persoonsgegevens weten wat hun verantwoordelijkheid is en hoe zij zorgvuldig om dienen te gaan met persoonsgegevens. Zij dienen in staat te zijn om te beoordelen welke gegevens nodig zijn voor het uitvoeren van de werkprocessen. Er dienen niet te weinig maar ook niet te veel gegevens te worden verwerkt (artikel 5.1c AVG). De FG zorgt samen met de CISO ervoor dat informatie over gegevensbescherming en informatieveiligheid herhaaldelijk onder de aandacht wordt gebracht van de voorzitter, leden en het secretariaat van de RKC. Medewerkers worden getraind in privacy-bewust functioneren door middel van presentaties, workshops en trainingen, door de leermodules in de e-learningomgeving.

4.3 Verplichte maatregelen en procedures

Om te voldoen aan de eisen van de AVG zijn de verplichte registers ingericht. Verder zijn onderstaande maatregelen getroffen:

- In het Informatiebeveiligingsbeleid zijn richtlijnen, primair op basis van de BIG en risico-gedreven, beschreven waaraan processen en informatiesystemen moeten voldoen om gegevensbescherming te borgen. Deze richtlijnen gelden voor proceseigenaren die nieuwe en bestaande processen en informatiesystemen beheren;
- Er is een procedure voor standaard incidentbeheer ingericht, de privacy incidentprocedure[4] sluit hier goed op aan. Dit vormt de basis voor *het Register van inbreuk op persoonsgegevens/datalekken;*
- Er is een procedure opgesteld waarin is vastgelegd hoe betrokkene(n) worden geïnformeerd bij een datalek;
- Alle gegevensverwerkingen waar persoonsgegevens worden verwerkt zijn in beeld gebracht en vastgelegd. Voor interne gegevensverwerkingen worden de gegevens opgeslagen en bijgehouden in het *Register van verwerkingen, met aantekeningen van PIA's;*
- Voor verwerkers worden de gegevens opgeslagen en bijgehouden in het *Register van verwerkersovereenkomsten, convenanten en privacy protocollen;*
- In het *Register voor aanvragen van betrokkenen* wordt bijgehouden welke aanvragen er zijn vanuit betrokkenen en het afhandelingstraject van de aanvraag.

4.4 Dataclassificatie

Met dataclassificatie wordt de uitvoering van het privacybeleid ondersteund op gebied van informatiebeveiliging. De maatregelen die getroffen moeten worden op gebied van informatiebeveiliging om de gegevensbescherming te kunnen borgen, zijn niet voor elk proces en informatiesysteem hetzelfde. Dit is de reden dat het nodig is dat alle processen en informatiesystemen die gegevens verwerken een eigen dataclassificatie ontvangen. Dataclassificatie heeft als doel om de *beschikbaarheid, integriteit en vertrouwelijkheid* van het proces en het informatiesysteem formeel te benoemen. Dit maakt inzichtelijk waarom maatregelen genomen moeten worden om de gegevens die verwerkt worden te beschermen. Elke proceseigenaar voorziet elk proces en informatiesysteem van dataclassificatie zoals deze is voorgeschreven vanuit de VNG door de Informatie Beveiligings Dienst[5] (Gemeenten IBD).

[4] Zie de procedure in Mozaiek: http://as-g-1mozaiekweb.sc.grid.internal/pls/dmoz/mozaiek/5406591
[5] http://www.binnenlandsbestuur.nl/Uploads/2014/2/13-1018-handreiking-dataclassificatie.pdf

4.5 Bewaren van gegevens

De AVG schrijft voor dat gegevens niet langer bewaard mogen worden dan noodzakelijk voor het doel waar ze voor nodig zijn. Dit doel wordt beschreven in verschillende wetten, daarom lopen de bewaartermijnen van persoonsgegevens uiteen. Daar waar er geen wettelijke bepaling is die voorziet in een verplichte bewaartermijn, dienen de RKC een eigen besluit over de bewaartermijn te nemen. Daarnaast geldt de Archiefwet voor het bewaren van papieren en elektronische documenten.

4.6 Delen van gegevens

Een rechtstreeks gevolg van het uitvoeren van wettelijke taken en - regelingen is het verwerken van persoonsgegevens. Een betrokkene moet daarom inzien dat wanneer er een melding of aanvraag gedaan wordt, dit gepaard gaat met verwerking van zijn/haar gegevens. Het is hierom van belang dat de RKC betrokkene informeert hoe zijn of haar gegevens worden verwerkt.
In sommige situaties kan het nodig zijn dat gegevens worden gedeeld. Het delen van deze gegevens wordt niet uitgevoerd zonder de expliciete toestemming van betrokkenen of wettelijke grondslag.

4.7 Open communicatie

Binnen de RKC is het belangrijk dat betrokkenen erop kunnen vertrouwen dat zijn of haar persoonsgegevens zorgvuldig worden verwerkt. Dat vertrouwen wordt gecreëerd door inzichtelijk te maken, door middel van verschillende communicatie kanalen, op welke wijze persoonsgegevens worden verwerkt en beheerd.

In privacy-protocollen worden aanleidingen gedocumenteerd en wordt inzichtelijk:
- welke gegevens worden verzameld;
- waarom deze gegevens worden verzameld;
- hoe deze gegevens worden verzameld en bewaard:
- wanneer en wat er vervolgens met deze gegevens gebeurt;
- wie toegang heeft tot deze gegevens;
- welke rechten inwoners en ondernemers hebben.

De bovenstaande lijst is niet uitputtend. Hiertoe zijn heldere, laagdrempelige procedures ingericht. Deze procedures worden, evenals de contactgegevens van de FG, gecommuniceerd naar betrokkenen. Betrokkenen worden zo gefaciliteerd in het doen van een beroep op één of meerdere van hun rechten. Processen en informatiesystemen die door de RKC worden gebruikt, zijn zodanig ingericht dat aan de vraag van betrokkenen kan worden voldaan (artikel 12 AVG).

4.8 Meldpunt datalekken

Bij een datalek kan gedacht worden aan het kwijtraken van een USB stick met persoons-gegevens, inbraak door een hacker, maar ook aan onbevoegde autorisaties in een informatiesysteem of informatie met, bijzondere, persoonsgegevens toegestuurd krijgen van de gemeente die niet voor de ontvanger is bestemd (brief of e-mail), het in de post zoekraken van een dossier. Ook het intern verwerken van te veel bijzondere persoonsgegevens is een datalek.

Wanneer er sprake blijkt van een inbreuk in verband met persoonsgegevens of te wel een datalek, moet dit datalek door de FG zonder vertraging worden gemeld aan de AP.

Een melding moet indien van toepassing ook onverwijld aan betrokkenen worden gedaan (artikel 33 AVG).
Om aan de wet te kunnen voldoen hanteert de RKC een procedure voor standaard incidentbeheer, de privacy-incidentprocedure welke hier goed op aansluit. Hierbij vormt de basis het verplichte Register van inbreuken op persoonsgegevens/datalekken.

Organisaties die persoonsgegevens verwerken zijn verplicht om datalekken binnen 72 uur na het ontdekken daarvan te melden bij de toezichthoudende organisatie, de AP. Het gaat hier om datalekken waar de organisaties voor verantwoordelijk zijn. Daaronder vallen ook datalekken die ontstaan bij een derde partij die werkzaamheden uitvoert voor de RKC.

De FG is gemandateerd door de RKC voor het melden van datalekken aan de AP.

Het melden van een, vermoedelijk, datalek door betrokkenen is mogelijk via de procedures zoals beschreven op de website van de RKC. Ook deze meldingen worden door de FG van de RKC gemeld bij de AP.
De AP is bevoegd om datalekken te beboeten en dwingende adviezen te geven ter verbetering van het zorgvuldig omgaan met persoonsgegevens.

4.9 Verwerkersovereenkomst

Bij veel gemeentelijke processen worden gegevens verwerkt door derden[6]. Denk hierbij naast werkzaamheden die uitgevoerd worden door leveranciers (van bijvoorbeeld Cloud-applicaties) ook aan het verrichten van onderzoeken door externe onderzoekbureaus. Het verlenen van opdrachten aan derden, verwerkers, brengt risico's met zich mee op het gebied van gegevensverwerking en informatieveiligheid. De RKC blijft verantwoordelijk voor de verwerking van de gegevens. Het afsluiten van verwerkersovereenkomsten geeft de mogelijkheid erop toe te zien dat ook door verwerkers gegevens juist worden beschermd en juist worden verwerkt[7]. Bij contracten waar persoonsgegevens door verwerkers worden verwerkt sluit de RKC de wettelijke verplichte verwerkersovereenkomsten af. In de verwerkersovereenkomsten worden minimaal afspraken gemaakt over:

- de doeleinden waarvoor de gegevens mogen worden verwerkt;
- hoe de verwerker met de persoonsgegevens moet omgaan;
- welke beveiligingsmaatregelen moeten worden genomen;
- welke vormen van toezicht de eigenaar mag uitoefenen;
- geheimhoudingsplicht;
- inschakeling van derden en onderaannemers;
- locatie van de data;
- aansprakelijkheid van schade door het niet naleven van regelgeving;
- exit-strategie.

Ten einde te borgen dat er verwerkersovereenkomsten worden gesloten, vormt dit een vast onderdeel in het inkoopproces. De verwerkersovereenkomsten worden opgenomen in het Register voor Verwerkersovereenkomsten.

[6] Zie artikel 4 AVG.
[7] Zie artikel 32 AVG.

5 Governance

5.1 Verantwoordelijken voor uitvoering en naleving AVG

De RKC is verantwoordelijk voor de juiste uitvoering van de AVG en naleving van het privacybeleid.
De door de RKC aangestelde FG zorgt voor onafhankelijk toezicht en controle op de kwaliteit van de uitvoering van het privacybeleid.

5.2 Verantwoording

Het dagelijks bestuur van de RKC zal binnen de jaarlijkse planning & control cyclus het algemeen bestuur informeren over de risico's en over de getroffen beheersmaatregelen op het gebied van privacy, binnen de processen waarvoor de RKC verantwoordelijk is.

Op grond van de AVG wordt de uitvoering van het privacybeleid elk jaar door de FG geauditeerd. De FG rapporteert aan het college van B & W en het Dagelijks Bestuur. Het afleggen van jaarlijkse verantwoording door de FG doet overigens niet af aan de algemene informatieplicht van het college en de burgemeester afzonderlijk[8], dan wel van het Dagelijks Bestuur.

5.2.1 Functionaris Gegevensbescherming

Voor onafhankelijk toezicht en controle op de kwaliteit van de uitvoering van het privacybeleid hebben de RKC een persoon aangesteld voor de functie van Functionaris Gegevensbescherming (FG)(artikel 37 AVG). Deze functie wordt gepositioneerd binnen het RKC. De FG heeft een onafhankelijke positie in de organisatie. De werkzaamheden die een FG uitvoert hebben een wettelijke grondslag[9].
De interne verantwoording is gewaarborgd door proceseigenaren binnen de RKC die rapporteren aan de FG over de realisatie van passende privacy-waarborgen. Zij rapporteren onverwijld bij privacy-incidenten conform de vastgestelde privacy-incidentprocedure.[10] Ook afwijkingen van de uitvoering van het privacybeleid worden direct gerapporteerd.
De FG ontwikkelt samen met de privacy coördinator een privacy-auditplan. De FG houdt toezicht op het uitvoeren van het auditplan en voert daarnaast zelfstandig controles uit. Het is de verantwoordelijkheid van de FG dat de RKC in control is en dat de registers op orde zijn. Ook in geval van calamiteiten moeten de procedures goed werken en dient de RKC in control te zijn. Het is de FG die toeziet op de prioritering van de processen en de wijze van implementatie van maatregelen.

De AVG verplicht tot het bijhouden van registers. Deze taken behoren toe aan de FG, bijgestaan door de privacy coördinator. De FG beheert de volgende verplichte registers:

- Register van verwerkingen, met aantekeningen van PIA's;
- Register van verwerkersovereenkomsten, convenanten en privacy protocollen;
- Register van inbreuken op persoonsgegevens, datalekken;
- Register voor aanvragen van betrokkenen.

De FG toetst de toepassing van het privacybeleid door de RKC. Zij treedt op als adviseur op beleidsniveau. De FG heeft, na formeel verzoek, het recht op toegang tot alle

[9] Zie artikelen 37 t/m 39 AVG.
[10] Zie de procedure in Mozaiek: http://as-g-1mozaiekweb.sc.grid.internal/pls/dmoz/mozaiek/5406591

informatie en systemen en processen waarin privacygegevens een rol (kunnen) spelen. De FG geniet ontslagbescherming en doet haar werk vrij van last en opdracht.

5.2.2 Privacy-coördinatoren

Privacy-coördinatoren zijn medewerkers binnen het secretariaat van de RKC. Zij zijn het interne aanspreekpunt voor de organisaties en communiceren en rapporteren aan/met de FG. Zij zijn in dienst van de RKC.
De Privacy coördinator onderzoekt voor elk proces met behulp van de procesrisicoanalyse of er sprake is van privacygevoelige gegevens. Indien geconstateerd is dat er sprake is van persoonsgegevens met een groot risico dient, eventueel in samenwerking met CIO Office, een PIA te worden uitgevoerd naar de risico's van het betreffende proces. Over alle, naar aanleiding van de uitkomst van de PIA genomen, maatregelen, wordt door de Privacy coördinator advies gevraagd aan de FG. De processen waar PIA's voor zijn uitgevoerd, worden periodiek geëvalueerd en de status wordt bijgewerkt in het register van verwerkingen van de FG.

Bij het in ontvangst nemen van verzoeken om inzage en informatie van betrokkenen speelt de Privacy coördinator een coördinerende rol. Daarnaast bewaakt zij de inzageprocessen en zal, indien van toepassing, opschalen naar de klachtenprocedure.

De Privacy coördinator zorgt ervoor dat betrokkenen met de FG contact kunnen opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van deze verordening.
Een belangrijk uitgangspunt in de AVG, waarop de AP zal gaan handhaven, is Accountability: de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van art. 5.1a AVG en kan deze aantonen (verantwoordingsplicht), artikel. 5.2 AVG.

In onderstaande tabel een overzicht van (op hoofdlijnen) de verantwoordelijkheden en bijbehorende verantwoordelijken betreffende uitvoering en invulling van de privacy wetgeving AVG.

Verantwoordelijkheid	Wie & hoe
Actief privacybeleid jegens betrokkenen	Proceseigenaren zijn verantwoordelijk voor correcte en transparante afwikkeling van de verzoeken van betrokkenen. Zij rapporteren hierover per aanvraag over de aanvraag en de afhandeling aan de FG. De FG ondersteunt proceseigenaren hierin en neemt de aanvraag en afhandeling op in het hiervoor bestemde register.
Actief privacybeleid medewerkers	De FG verzorgt samen met de proceseigenaren training van en toezicht op privacy-bewustzijn van de medewerkers.
Actief privacybeleid jegens verwerkers	Daar waar verwerkingen uitbesteed worden aan derden zijn de proceseigenaren verantwoordelijk voor het sluiten van verwerkersovereenkomsten. Proceseigenaren rapporteren hierover aan de FG. De FG beheert de afgesloten verwerkersovereenkomsten in het verplichte register van verwerkersovereenkomsten.
Beheer van het beleid	De FG beheert het beleid. De FG rapporteert aan de raadsgriffier, over de voortgang en de kwaliteit van de uitvoering, en doet aanbevelingen voor verdere optimalisering. Waarborg voor optimalisering is het hanteren van de PDCA-cyclus.
Bestuurlijke verantwoording	Jaarlijks legt het college van B&W verantwoording af aan de Gemeenteraad over de risico's en beheersmaatregelen. Het Dagelijks bestuur legt verantwoording af aan het Algemeen bestuur.
Interne verantwoording	De FG rapporteert ieder kwartaal aan de Voorzitter, leden en het secretariaat van de RKC. Indien proceseigenaren verantwoordelijkheden hebben overgedragen, dragen zij zorg voor een gelijkwaardige vorm van verantwoording en voor kennisgeving hiervan aan de FG.
Praktische privacy waarborgen	Concretiseren van praktische privacy waarborgen gebeurt onder verantwoordelijkheid van de proceseigenaar.
Privacy- auditplan	De FG ziet er samen Privacy Coördinator op toe dat er een privacy-auditplan ontwikkeld wordt en dat dit wordt uitgevoerd door o.a. de Privacy Coördinator. Dit plan wordt jaarlijks opgesteld en is in lijn met het Raamwerk privacy-audit van de AP. De PDCA-cyclus wordt hierop toegepast.
Risico gedreven aanpak	Vertrekpunt voor het maken van beleidskeuzes is de PIA. Na advies van de FG wordt de mate van persoonlijk - en bestuurlijk risico in kaart gebracht. De risico's worden door praktische -, organisatorische - en technische maatregelen beheerst en volgens de PDCA-cyclus geborgd.
Toezicht	De RKC heeft een Functionaris Gegevensbescherming (FG) aangesteld (artikelen 37 t/m 39 AVG). De FG rapporteert aan gemeente secretaris en onderhoudt de contacten met de AP.
Uitvoering van privacybeleid	Functionaris Gegevensbescherming (FG) is verantwoordelijk voor uitvoering van het beleid en voor controle op de naleving van het privacybeleid.
Vaststellen privacybeleid	Voorzitter, leden en het secretariaat van de RKC hebben het beleid vastgesteld en bevorderen de beschikbaarheid van voldoende middelen om privacybescherming passend te waarborgen.
Verantwoording PIA's en verantwoordelijkheid voor audits	De FG ziet in overleg met de proceseigenaren toe op de controle van de uitvoering van de op basis van PIA's uitgevoerde maatregelen. Daarnaast ziet de FG toe op de

	ontwikkeling en uitvoering van een privacy-auditplan samen met de Privacy Coördinator. Aan de hand hiervan kan de PDCA-cyclus worden doorlopen waarmee continu verbeteren wordt geborgd.

In onderstaand overzicht zijn de taken (op hoofdlijnen) beschreven van alle bij de privacybescherming betrokken functionarissen.

Functie	Taak
Voorzitter, leden en het secretariaat van de RKC	Vaststellen privacybeleid.
Functionaris Gegevensbescherming	Zorgdragen voor ontwikkeling en beheer van wettelijk verplichte registers; Houdt toezicht op en coördineert de uitvoering van het auditplan en voert daarnaast zelf controles uit; Ziet toe op het toewijzen van verantwoordelijkheden, privacy-awareness en het opleiden van collega's; Adviseert over het uitvoeren van Privacy Impact Assessments (PIA) en houdt toezicht op de uitvoering; Zorgdragen voor en toezicht houden op de training van medewerkers op het gebied van privacy-bewustzijn; Adviseert organisaties hoe te handelen rond incidenten m.b.t. het privacybeleid (o.a. datalekken); Zorgdragen voor verantwoordingsrapportages aan het bestuur per kwartaal; Melden van datalekken bij AP.
Voorzitter, leden en het secretariaat van de RKC de Proceseigenaren	Toezien op het in behandeling nemen en correct afhandelen van verzoeken om inzage en informatie van betrokkenen; Training van en toezicht op privacy bewustzijn van medewerkers; Kwartaalrapportages aan FG; Melding van datalekken bij FG.
Privacy-coördinatoren	Opbouwen en onderhouden van privacy deskundigheid binnen de afdeling (structureel); Adviseren over eenvoudige ad-hoc privacy vraagstukken die de afdeling betreffen; Uitvoeren van het beleid binnen de afdeling; Meewerken aan het opstellen en bewaken van afdelingsspecifieke werkinstructies; Ontwikkelen van afdelingsspecifieke handreikingen voor professionals; Eerste aanspreekpunt voor de voorzitter van de RKC betreffende privacy; Ondersteuning bij het beantwoorden van Raadsvragen; Het in ontvangst nemen van verzoeken om inzage en informatie van betrokkenen; Zorgt ervoor dat betrokkenen met de FG contact kunnen opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van deze verordening;

	Coördineert en bewaakt inzageprocessen, zo nodig, signaleren en opschalen naar klachtenprocedure (incidenteel); Meewerken aan onderzoeken (incidenteel); Verantwoordelijk voor het verzamelen van informatie ten behoeve van data-inventarisaties; Voorbereiden van informatie voor meldingen van gegevensverwerking (melding wordt gedaan door FG); Collega's actief wijzen op de meldplicht (kennissessies), signalen oppakken en doorzetten; Informeert de FG naar behoren en tijdig bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. (structureel)(artikel 38 lid 1 AVG); Mee reviewen van externe communicatie over privacy en gezamenlijke belangen bewaken; Controleren/ aanvullen register van verwerkingsactiviteiten; Voorbereiding en eventueel opstellen van convenanten en verwerkersovereenkomsten; Kennis nemen van relevante privacy-ontwikkelingen; Autorisatie matrices mee beoordelen en controleren; Signaleren van afwijkingen in de afspraken rondom gegevensverwerkingen in datasystemen; Bijdrage leveren aan control van privacy; Verantwoordelijk voor de informatieverstrekking in het kader van audits en mede aanspreekpunt voor de auditcommissie; Voor zover er sprake is van een afdelingsspecifieke audit, deze uitvoeren en mee ontwikkelen; Wint advies in bij de FG bij PIA's/ gegevensbeschermingseffectbeoordeling Uitvoeren van PIA's (privacy impact assessments) op bestaande werkprocessen; Dient onder aansturing door de FG o.a.: • *Het Register van Verwerkingen te controleren en beheren;* • *Toe te zien op invulling, door afdeling contractmanagement, van het Register van verwerkingsovereenkomsten;* • *Het Register van Rechten betrokkenen te controleren en beheren;* • *Het Register voor het melden van inbreuken op de persoonsgegevens (datalekken)te maken en bijhouden;* • *Hierbij hoort ook dossiervorming van de achterliggende stukken;*