



PRIVACYBELEID REKENKAMER DORDRECHT

Privacybeleid van de Rekenkamer Dordrecht bij de voorbereiding, uitvoering en publicatie van haar onderzoeken. Vastgesteld in haar vergadering van 12 december 2023



Inleiding

Gemeenten en gemeentelijke organisaties verwerken persoonsgegevens om een dienst te verlenen, een product te leveren of om andere doelen te bereiken. Het verwerken van persoonsgegevens levert altijd in meer of mindere mate een inbreuk op het recht op gegevensbescherming of de persoonlijke levenssfeer van burgers op. Deze inbreuken dienen altijd gerechtvaardigd te zijn en hieraan gaat dan ook altijd een belangenafweging aan vooraf waarbij tevens wordt beoordeeld op welke wijze de gegevensverwerking in lijn met de geldende wet- en regelgeving op het gebied van gegevensbescherming (hierna privacywetgeving) kan plaatsvinden.

Het is een wettelijke verplichting dat overheidsorganisaties behoorlijk, zorgvuldig en transparant omgaan met persoonsgegevens. Middels dit privacybeleid geeft de Rekenkamer van de gemeente Dordrecht invulling aan de verplichtingen die volgen uit de privacywetgeving. Dit privacybeleid staat niet op zichzelf, ook de regio Drechtsteden heeft privacybeleid¹ geformuleerd, waarin beschreven staat hoe om te gaan met de verwerking van persoonsgegevens. Binnen de gemeente Dordrecht is dit privacybeleid van toepassing. De Rekenkamer Dordrecht (hierna RK Dordrecht) conformeert zich derhalve aan het geformuleerde privacybeleid van de gemeente Dordrecht.

Dit document beschrijft de kaders voor het verwerken van persoonsgegevens, de bescherming van deze gegevens en omgang met deze gegevens. Dit beleid dient als kapstok of leidraad om werkprocessen in te richten zodat in de praktijk aan de privacywetgeving wordt voldaan bij de uitvoering van de werkzaamheden van de RK Dordrecht.

De werkzaamheden van de RK Dordrecht betreffen onderzoeken naar de doelmatigheid, doeltreffendheid en rechtmatigheid van het door het gemeentebestuur gevoerde bestuur. Meestal is het voor die onderzoeken nodig om gewone persoonsgegevens zoals contactgegevens te verwerken. In specifieke onderzoeken is het soms noodzakelijk om gevoelige of bijzondere persoonsgegevens te gebruiken, denk aan gezondheidsgegevens, culturele achtergrond, inkomensgegevens. Voorafgaand aan elk onderzoek weegt de RK Dordrecht 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. Denk aan IT-beveiligingsmaatregelen om informatie te beschermen tegen indringers van buitenaf, het toepassen van encryptie en het toepassen van authenticatie- en autorisatiebeleid voor de toegang tot informatie. Voor het borgen van de bescherming van persoonsgegevens is het naleven van wat is geregeld in het Informatiebeveiligingsbeleid Drechtsteden² dan ook van cruciaal belang.

De Autoriteit Persoonsgegevens (verder te noemen AP) is de externe toezichthouder op een behoorlijke, zorgvuldige en transparante verwerking van persoonsgegevens binnen Nederlandse organisaties, waaronder overheden.

¹ [Informatiesysteem Gemeente Dordrecht - Dossier - 2610764](#)

² [Link naar Informatiebeveiligingsbeleid gemeente](#)



1. Uitgangspunten

1.1. Doelstellingen van het beleid

Doelstelling van het beleid is dat binnen de RK Dordrecht op een verantwoordelijke wijze en binnen wettelijke kaders met persoonsgegevens wordt omgegaan. Het wettelijke kader voor bescherming van persoonsgegevens wordt, naast specifieke wetten, aangegeven door de Algemene Verordening Gegevensbescherming (hierna AVG). De eisen die de AVG stelt aan het verwerken van persoonsgegevens zijn dan geïmplementeerd bij de RK Dordrecht. Als startpunt is het verplichte bewustwordingsprogramma voor alle medewerkers opgezet. Bewustwording en bewustzijn vormt de basis voor de verdere professionalisering binnen de RK Dordrecht.

De RK Dordrecht wil onder andere hiermee bereiken dat:

- de basis voor een goed geïmplementeerd privacybeleid wordt gegarandeerd;
- de rechten van betrokkenen worden gerespecteerd en in procedures zijn verankerd;
- het vertrouwen van burgers in de overheid niet wordt beschaamd; uitvoering van het privacybeleid binnen de RK Dordrecht gericht wordt opgepakt, zodat de wettelijke eisen goed geïmplementeerd zijn;
- het onderwerp breed wordt gedragen binnen de RK Dordrecht, als onderdeel van zowel uitvoering van de wettelijke opgave, goed werkgeverschap en opdrachtgeverschap;
- de kans op datalekken klein is waardoor financiële schade door het oplopen van boetes van de AP en reputatieschade wordt geminimaliseerd.

1.2. Begrippenkader

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

Accountability: Verantwoording kunnen afleggen op welke manier uitvoering is gegeven aan de verplichtingen die de AVG stelt aan de verwerking van persoonsgegevens.

Algemeen Bestuur RK (AB RK Dordrecht): Voorzitter, commissieleden RK Dordrecht.

Betrokkene: De natuurlijke persoon van wie de gegevens worden verwerkt.

Datalek: Een inbreuk op de beveiliging waardoor al dan niet per ongeluk persoonsgegevens op onrechtmatige wijze worden verwerkt. Bijvoorbeeld vernietiging, verlies, onbedoelde wijziging, ongeoorloofde verstrekking of ongeoorloofde toegang tot persoonsgegevens.

Datalekprocedure: De RK Dordrecht heeft een procedure om beveiligingsincidenten met persoonsgegevens te melden en af te handelen zodat kan worden voldaan aan de registratie en eventueel de meldingsplicht bij de AP bij ernstige datalekken.

DPIA (light): Methode om de effecten en risico's van nieuwe of bestaande verwerkingen op de bescherming van de privacy te beoordelen.

Functionaris Gegevensbescherming (hierna FG): De RK Dordrecht heeft een eigen interne onafhankelijke FG die de RK Dordrecht adviseert en controle houdt op de naleving van de verplichtingen uit de AVG.



Governance: De wijze waarop binnen de RK Dordrecht verantwoordelijkheid ten aanzien van de daadwerkelijke uitvoering van richtlijnen en beleid is gegarandeerd, zodat vereiste processen op de juiste manier worden gevolgd om te kunnen voldoen aan AVG. Governance bevat het definiëren van rollen en verantwoordelijkheden, meten, rapporteren en het nemen van acties om geïdentificeerde kwesties op te lossen.

Passende technische - en organisatorische maatregelen: IT-beveiligingsmaatregelen die gelden binnen de gemeente Dordrecht zijn bekend en worden toegepast. De RK Dordrecht legt schriftelijke afspraken vast over de verplichtingen uit de AVG met onderzoeksbureaus en andere partijen;

Persoonsgegevens Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene) als bedoeld in de AVG.

Bijzondere persoonsgegevens: gegevens over ras/etniciteit, religie, politieke voorkeur, lidmaatschap van vakbond, gezondheid, biometrische gegevens ter identificatie, genetische gegevens en gegevens over seksuele leven.

Privacybescherming: Het omgaan met persoonsgegevens conform de normen in de AVG.

Datalekprocedure: De RK Dordrecht heeft een procedure om beveiligingsincidenten met persoonsgegevens te melden en af te handelen zodat kan worden voldaan aan de registratie en eventueel de meldingsplicht bij de AP bij ernstige datalekken.

Secretariaat RK Dordrecht: de ondersteuning vanuit de Raadsgriffie Dordrecht aan de Rekenkamer Dordrecht.

Verantwoordingsplicht: Het bijhouden van een register van verwerkingsactiviteiten en de uitvoering van de Quickscan Data Protection Impact Assessment (hierna DPIA), de uitvoering van een DPIA light/ DPIA.

Verwerking: Een handeling of een geheel van handelingen met betrekking tot 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.

Verwerkingsverantwoordelijke: 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.

1.3. Juridisch kader - basisbeginselen 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 vergaande inbreuken op het recht op gegevensbescherming en het recht op bescherming van de persoonlijke levenssfeer 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 AVG kent een aantal basisbeginselen waaraan de RK Dordrecht op de volgende wijzen uitvoering geeft:

- Verwerking van persoonsgegevens gebeurt op rechtmatige, behoorlijke en transparante wijze (artikel 5, lid 1 (a) AVG);
- Persoonsgegevens worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 5, lid 1 (b) AVG);
- Wees kritisch en verzamel alleen die persoonsgegevens die noodzakelijk zijn voor het doel (dataminimalisatie) (artikel 5, lid 1 (c) AVG);
- Zorg ervoor dat met juiste gegevens wordt gewerkt en maak het mogelijk dat onjuiste gegevens zo snel mogelijk worden gecorrigeerd (artikel 5, lid 1 (d) AVG)
- Verwijder gegevens, zodra die niet meer nodig zijn. Onderzoeksgegevens die de RK Dordrecht gebruikt, worden niet oneindig bewaard (artikel 5, lid 1 (e) AVG). Met onderzoeksbureaus worden schriftelijke afspraken gemaakt over de verwijdering van gegevens.
- De RK Dordrecht treft IT-maatregelen om gegevens te beschermen tegen datalekken en neemt organisatorische maatregelen zoals trainingen, toegangsbeperkingen om datalekken te voorkomen (artikel 5, lid 1 (f) AVG)
- De RK Dordrecht kan te allen tijde verantwoording afleggen aan burgers en de AP over de keuzes die zijn gemaakt bij de verwerking van gegevens. De RK Dordrecht zorgt ervoor dat de motivering bij de keuzes wordt gedocumenteerd, zodat hierop kan worden teruggegrepen indien nodig (artikel 5, lid 2 AVG).
- De RK Dordrecht verwerkt persoonsgegevens op basis van tenminste één van de in de AVG opgenomen grondslagen (artikel 6 AVG) en stelt deze grondslag(-en) voor aanvang van de gegevensverwerking vast.
- De RK Dordrecht stelt burgers via de privacyverklaring op de website op de hoogte van de soort gegevensverwerkingen die onder verantwoordelijkheid van de RK Dordrecht worden uitgevoerd en zorgt ervoor dat burgers eenvoudig hun privacyrechten kunnen uitoefenen (Hoofdstuk III AVG).

Van belang is dat persoonsgegevens worden verwerkt voor vooraf bepaalde, gerechtvaardigde, duidelijk omschreven doeleinden. Naast gerechtvaardigde doeleinden dient iedere gegevensverwerking gebaseerd te worden op één of meer limitatief genoemde grondslagen uit de AVG. Vervolgens moet worden beoordeeld dat de gegevensverwerking proportioneel en subsidiair is. Dit betekent een beoordeling en motivering dat de inbreuk als gevolg van de gegevensverwerking in evenredige verhouding staat tot het doel dat ermee wordt beoogd, en dat goed is nagedacht over alternatieve oplossingen om dat doel te bereiken die een minder grote inbreuk opleveren. Er moet dan gekozen worden voor de oplossing die de minste inbreuk oplevert voor het recht op gegevensbescherming van betrokkene.

Het verwerken van bijzondere persoonsgegevens vergt een stringente beoordeling op noodzakelijkheid en evenredigheid. De RK Dordrecht kan gegevens die voor een andere doeleinde op een eerder moment zijn verzameld voor onderzoeksdoeleinden gebruiken en past daarbij passende maatregelen toe om gegevensbescherming te garanderen. Zo zal in verreweg de meeste



gevallen onderzoeksgegevens op pseudonieme wijze worden verzameld. Burgers kunnen altijd inzage of wijziging van de verwerkte persoonsgegevens opvragen. De RK Dordrecht heeft een eigen FG waar burgers terecht kunnen bij klachten over de wijze waarop de RK Dordrecht gegevens verwerkt.

De RK Dordrecht heeft de wettelijk verplichting om gegevensbescherming te borgen. Dit moet zij doen door technische en organisatorische maatregelen te treffen. Informatiebeveiliging is hier een groot onderdeel van. Samen met onder andere informatiebeheer, het juridische kader en privacybewustzijn zorgt informatiebeveiliging voor de borging van bescherming van persoonsgegevens. Voor de informatiebeveiliging maakt de RK Dordrecht gebruik van de diensten op ICT-gebied binnen de gemeente Drechtsteden. Er wordt gewerkt binnen de kaders van het Informatiebeveiligingsplan en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

De AVG en de Uitvoeringswet AVG bevatten de belangrijkste juridische kaders van de gegevensbeschermingswetgeving voor de RK Dordrecht. Daarnaast zijn er diverse specifieke wetten, zoals de Wet Basisregistratie Personen, de Wet Maatschappelijke Ondersteuning, de Jeugdwet en de Wet politiegegevens, die van toepassing kunnen zijn in specifieke onderzoekssituaties en aanvullende eisen kunnen stellen aan de verwerking van gegevens die onder deze wetgeving vallen. Deze wetten worden in dit beleidsstuk niet verder uitgewerkt.

1.4. Wijze van inrichten gegevensverwerking

Het onderwerp privacy wordt indien nodig op de vergaderagenda's van de RK Dordrecht geplaatst. Dit gebeurt in ieder geval bij nieuwe onderzoeken én ieder halfjaar om de voortgang van de werkzaamheden die voortvloeien uit de GAP-analyse te bespreken. Hierdoor ontstaat een continue proces van veranderen en verbeteren.

Om de RK Dordrecht te ondersteunen zijn experts ingezet op het gebied van gegevensverwerking en informatiebeveiliging³. Deze experts werken zoveel mogelijk met elkaar samen.

1.5. Doelgroep

Het privacybeleid voor de RK Dordrecht is kaderstellend op alle taken en processen waar de RK Dordrecht voor verantwoordelijk is. Dit privacybeleid en een juiste uitvoering hiervan richt zich tot alle interne en externe medewerkers en opdrachtnemers⁴ van de RK Dordrecht. Het is vooral gericht op diegenen die werken met persoonsgegevens, dan wel persoonsgegevens laten verwerken door externe partners, zoals onderzoeksbureau's. De voorzitter, leden en het secretariaat spelen een belangrijke rol bij de besluitvorming over dit onderwerp en de sturing ervan in de PDCA-cyclus.

1.6. Ingangsdatum

Dit privacybeleid is van kracht per 1 januari 2024 en vervangt het privacybeleid dat is vastgesteld op 17 juni 2019.

³ Het gaat hier om de FG van de RK Dordrecht en de FG van de gemeente Dordrecht en de CISO van de gemeente Dordrecht.

⁴ Denk aan onderzoeksbureaus die de RK Dordrecht inzet.



2. Rechten van betrokkenen

De AVG verleent burgers privacyrechten. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt 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. Burgers hebben de volgende rechten:

- informatie over de gegevensverwerkingen (artikel 13 en 14 AVG)
- inzage van gegevens (artikel 15 AVG);
- rectificatie van gegevens (artikel 16 AVG);
- gegevenswissing, recht op "vergetelheid" (artikel 17 AVG);
- beperking van de verwerking (artikel 18 AVG);
- kennisgevingplicht inzake rectificatie, wissing of beperking (artikel 19 AVG);
- overdraagbaarheid van gegevens, dataportabiliteit (artikel 20 AVG); en
- het recht om niet te worden onderworpen aan automatische besluitvorming zonder menselijke tussenkomst (artikel 21 AVG).

2.1. Recht op informatie (artikel 13 en 14 AVG)

Burgers hebben recht om te weten wat een organisatie met hun gegevens doet. De RK Dordrecht geeft invulling aan het recht op informatie door de plaatsing van de privacyverklaring op de website van de RK Dordrecht. Indien mogelijk worden burgers individueel geïnformeerd over de verwerking van hun gegevens in onderzoeken van de RK Dordrecht middels bijvoorbeeld deelnemersinformatie. De informatie bevat tenminste de doeleinden van de verwerking, de soort gegevens die worden verwerkt, de grondslag waarop dit is gebaseerd, wie de gegevens tot hun beschikking krijgen, hoe lang de gegevens worden bewaard, op welke wijze burgers hun rechten kunnen uitoefenen en de contactgegevens van de FG van de RK Dordrecht.

2.2. Recht op inzage van gegevens (artikel 15 AVG)

Naast het recht op informatie hebben burgers het recht om inzage te verkrijgen van de persoonsgegevens die de RK Dordrecht van hen verwerkt. Tevens hebben zij recht op uitleg over waarom en hoe hun persoonsgegevens worden verwerkt. Hierbij kan de RK Dordrecht eisen dat een burger zich identificeert. Hiermee wordt terughoudend omgegaan. 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.

2.3. Recht op rectificatie van gegevens (artikel 16 AVG)

Burgers hebben het recht om van de verwerkingsverantwoordelijke onverwijld een rectificatie van hen 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 aan te vullen. Dit artikel is een verdere uitwerking van artikel 5, lid 1, sub d, het beginsel van juistheid van persoonsgegevens. De RK Dordrecht en eventueel ingeschakelde onderzoeksbureaus moeten alle redelijke maatregelen nemen om ervoor



te zorgen dat onjuiste persoonsgegevens worden gerectificeerd. Het is daarbij irrelevant of de onjuistheden berusten op een fout van de RK Dordrecht of het onderzoeksbureau.

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

Burgers hebben het recht op wissing van hen betreffende persoonsgegevens. De RK Dordrecht is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer aan de voorwaarden voor gegevenswissing wordt voldaan. De AVG kent een uitzonderingsbepaling indien gegevens met het oog op onderzoek worden verwerkt. De RK Dordrecht gaat terughoudend met deze uitzonderingsbepaling om en kijkt steeds per individueel geval of toepassing van de uitzonderingsbepaling noodzakelijk is, bijvoorbeeld omdat gegevenswissing de onderzoeksdoeleinden kan frustreren. Er vindt een belangenafweging plaats.

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 RK Dordrecht en eventueel ingeschakelde onderzoeksbureaus.

2.5. Recht op beperking van de verwerking (artikel 18 AVG)

De betrokkene heeft het recht van de RK Dordrecht de beperking van de verwerking te verkrijgen. Beperking is gedefinieerd 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.

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

De RK Dordrecht stelt iedere ontvanger (niet zijnde betrokkene, bijvoorbeeld een onderzoeksbureau) 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 dit onevenredig veel inspanning vergt. De RK Dordrecht verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.

Wanneer de RK Dordrecht een rectificatie (artikel 16 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.

2.7. Recht op overdraagbaarheid gegevens, dataportabiliteit (artikel 20 AVG)

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. Gelet op de aard van de gegevensverwerkingen door de RK Dordrecht zal dit recht niet snel aan de orde zijn.



2.8. Recht om niet te worden onderworpen aan automatische besluitvorming zonder menselijke tussenkomst (artikel 21 AVG)

De AVG kent burgers het recht toe om niet onderworpen te worden aan geautomatiseerde individuele besluitvorming zonder menselijke tussenkomst. Hieronder valt ook profilering. Het gaat om geautomatiseerde besluiten of een geautomatiseerde evaluatie van persoonlijke aspecten van burgers waarmee beroepsprestaties, de economische situatie, gezondheid, persoonlijke voorkeuren, gedrag, locatie of verplaatsingen worden geanalyseerd of voorspeld. Deze besluiten moeten wel rechtsgevolgen kunnen hebben voor burgers of dusdanige gevolgen waardoor zij in aanmerkelijke zin worden getroffen. Dit recht heeft betrekking op besluiten die geautomatiseerd worden genomen door middel van computers of met behulp van algoritmen. Wil een organisatie toch dergelijke geautomatiseerde besluiten nemen dan kunnen burgers daarvoor toestemming geven of de mogelijkheid voor het nemen van dergelijke besluiten moet zijn vervat in een wettelijke grondslag. De RK Dordrecht neemt geen besluiten die individuele burgers treffen. Ook worden er geen profielen gemaakt van burgers die rechtsgevolgen hebben of die voor hen op een andere wijze een nadelig effect kunnen hebben. Daarom zal inroeping van dit recht niet snel aan de orde zijn.



3. Werkprocessen

3.1. Omgaan met persoonsgegevens

Persoonsgegevens worden door de RK Dordrecht alleen verwerkt voor het uitvoeren van de wettelijke taken van de RK Dordrecht: het onderzoeken van de doeltreffendheid, doelmatigheid en rechtmatigheid van het gemeentelijke beleid. (Zie ook paragraaf 2.3 Juridisch kader.) In het merendeel van de gevallen worden persoonsgegevens aan de RK Dordrecht door burgers of andere onderzoekdeelnemers zelf verstrekt.

De RK Dordrecht verwerkt voor haar onderzoeken soms ook persoonsgegevens die bij de gemeente of een gemeentelijke instelling worden opgevraagd. Zij zijn op grond van de Gemeentewet⁵ verplicht deze gegevens aan de RK Dordrecht te verstrekken en de burgers daarover te informeren. Deze gegevens laat de RK Dordrecht verwerken zonder de burger daarover nog afzonderlijk te informeren. De RK Dordrecht kan zich hiervoor beroepen op de uitzonderingsbepaling van artikel 14, lid 5 onder c, van de AVG. De analyse van deze gegevens worden gebruikt in rapporten van de RK Dordrecht. De gebruikte persoonsgegevens worden niet openbaar gemaakt of met anderen gedeeld.

Ook komt het voor dat de RK Dordrecht de betrokkene om persoonsgegevens vraagt, bijvoorbeeld via een enquête, een interview of een groepsgesprek. Sporadisch kan het voorkomen dat de RK Dordrecht burgers om bijzondere persoonsgegevens zal vragen (zoals gezondheidsgegevens). Dit kan aan de orde zijn als de RK Dordrecht een onderzoek (laat) doen in het sociaal domein. Ook kan het voorkomen dat de RK Dordrecht toestemming aan burgers vraagt om een (deel) van het gemeentelijk dossier, waarin bijzondere persoonsgegevens staan, te mogen betrekken bij een onderzoek. De (bijzondere) persoonsgegevens worden pas door de RK Dordrecht verzameld als de betrokkene daarmee expliciet akkoord is gegaan. Ook voor deze persoonsgegevens geldt dat de RK Dordrecht deze niet openbaar maakt.

Alleen met uitdrukkelijke toestemming van onderzoekdeelnemers neemt de RK Dordrecht naam en functie van betrokkene op in haar rapport. Van politici die verbonden zijn aan de gemeente Dordrecht registreert de RK Dordrecht 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 RK Dordrecht nemen wij een zo groot mogelijke spreiding van politieke overtuiging in acht.

De RK Dordrecht verwerkt gegevens in informatiesystemen. Deze informatiesystemen zijn in beheer van de Gemeente Dordrecht. Het secretariaat wint, voor zover nodig, advies in van de FG en de CISO van de gemeente Dordrecht.

⁵ Zie artikel 183 Gemeentewet.



3.2. Bewustwording

Zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren en naleven van normen op het gebied van informatiebeveiliging 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 persoonsgegevens 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. Het secretariaat zorgt ervoor op de hoogte te blijven van gegevensbescherming en informatieveiligheid middels trainingen over privacybewust functioneren door middel van presentaties, workshops en trainingen, en e-learnings die door de gemeente Dordrecht aan medewerkers worden aangeboden.

3.3. Verplichte maatregelen en procedures

De RK Dordrecht heeft onderstaande maatregelen getroffen:

- De RK Dordrecht heeft een register van verwerkingsactiviteiten ingericht waarin alle gegevensverwerkingen, zoals onderzoeken waarmee met persoonsgegevens wordt gewerkt, zijn geregistreerd.
- De RK Dordrecht heeft een datalekregister waarin alle gemelde datalekken worden geregistreerd.
- De RK Dordrecht werkt aan een datalekprocedure voor het melden en afhandelen van datalekken. Hierin wordt vastgelegd of en hoe betrokkene(n) worden geïnformeerd bij een datalek.
- De RK Dordrecht volgt het informatiebeveiligingsbeleid van de gemeente Dordrecht. Deze richtlijnen gelden voor de werkprocessen bij de uitvoering van de wettelijke taken van de RK Dordrecht. De RK Dordrecht bepaalt de waarde van informatie door deze te toetsen aan de BIV-classificatie en treft vervolgens de nodige maatregelen.
- Voor verwerkers worden de gegevens opgeslagen en bijgehouden in het register van verwerkersovereenkomsten;
- In het register voor aanvragen van betrokkenen worden bijgehouden welke aanvragen er zijn vanuit betrokkenen en het afhandelingstraject van de aanvraag.

3.4. Bewaren van gegevens

De AVG schrijft voor dat gegevens niet langer bewaard mogen worden dan noodzakelijk voor het doel waarvoor ze 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, dient de RK Dordrecht een eigen besluit over de bewaartermijn te nemen. Daarnaast geldt de Archiefwet 1995 voor het bewaren van papieren en elektronische documenten.

3.5. Delen van gegevens

In uitzonderlijke situaties kan het nodig zijn dat de RK Dordrecht gegevens deelt. Het delen van deze gegevens wordt niet uitgevoerd zonder de expliciete toestemming van betrokkenen of een andere wettelijke grondslag.

3.6. Open communicatie

De RK Dordrecht vindt het belangrijk dat burgers erop kunnen vertrouwen dat zijn of haar persoonsgegevens zorgvuldig worden verwerkt. Dat vertrouwen wordt gecreëerd door inzichtelijk te maken op welke wijze persoonsgegevens worden verwerkt en beheerd.

In de privacyverklaring van de RK Dordrecht is daarom informatie te vinden over:

- welke gegevens worden verwerkt;
- 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. Betrokkenen worden ook gefaciliteerd in het doen van een beroep op één of meerdere van hun rechten. Processen en informatiesystemen die door de RK Dordrecht worden gebruikt, zijn zodanig ingericht dat aan de vraag van betrokkenen kan worden voldaan (artikel 12 AVG).

3.7. Meldpunt datalekken

Een datalek wordt in de AVG omschreven als 'een inbreuk in verband met persoonsgegevens'. In de volksmond wordt een dergelijke inbreuk een datalek genoemd. Een datalek is een beveiligingsincident waarbij persoonsgegevens betrokken zijn. Het moet dus gaan om een inbreuk op bestaande beveiligingsmaatregelen, waardoor daadwerkelijk persoonsgegevens zijn verloren gegaan, zijn gestolen, of waardoor onbevoegden toegang hebben gekregen tot de persoonsgegevens. Daaronder vallen ook datalekken die ontstaan zijn bij een derde partij die werkzaamheden uitvoert voor de RK Dordrecht, zoals onderzoeksbureaus. Men kan daarbij denken aan het kwijtraken van een USB-stick met persoonsgegevens, inbraak door een hacker, maar ook aan onbevoegde autorisaties in een informatiesysteem of het verzenden van persoonsgegevens aan verkeerde ontvangers.

Wanneer er sprake blijkt van een ernstig 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 RK Dordrecht datalekprocedure. In deze procedure is beschreven hoe de melding en beoordeling van het datalek plaatsvindt. Deze beoordeling betreft de mate van ernst van het datalek en de afweging of het datalek gemeld moet worden aan de AP en wie op welk moment bij deze beoordeling betrokken wordt.

De RK Dordrecht is verplicht om ernstige datalekken binnen 72 uur na het ontdekken daarvan te melden bij de AP. Ieder datalek wordt geregistreerd in het verplichte register van datalekken. Het maakt daarvoor niet uit of het om een ernstig datalek gaat of om een datalek dat niet gemeld hoeft te worden bij de AP.

De FG is gemandateerd door de RK Dordrecht voor het melden van datalekken aan de AP. Het melden van een al dan niet vermoedelijk, datalek door burgers of andere ontdekkers, is mogelijk via de procedure zoals beschreven in de privacyverklaring van de RK Dordrecht.

3.8. Verwerkersovereenkomst

De RK Dordrecht laat veel onderzoeken uitvoeren door onderzoeksbureaus. Het verlenen van opdrachten aan derden / verwerkers brengt risico's met zich mee op het gebied van gegevensverwerking en informatieveiligheid. De RK Dordrecht blijft verantwoordelijk voor de verwerking van de gegevens. Het afsluiten van verwerkersovereenkomsten geeft de mogelijkheid erop toe te zien dat ook door verwerkers gegevens op een juiste wijze worden beschermd en op een juiste wijze worden verwerkt. Bij contracten waar persoonsgegevens door verwerkers worden verwerkt sluit de RK Dordrecht de verplichte verwerkersovereenkomsten af. In de verwerkersovereenkomsten worden tenminste 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 de opdrachtverstrekking. De verwerkersovereenkomsten worden opgenomen in het register voor verwerkersovereenkomsten.



4. Governance

Verantwoordelijken voor uitvoering en naleving AVG

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

4.1. Verantwoording

Op grond van de AVG wordt de uitvoering van het privacybeleid door de RK Dordrecht elk jaar door de FG gemonitord aan de hand van de geformaliseerde GAP-analyse. De FG rapporteert de uitkomsten van de GAP-analyse aan het AB RK Dordrecht.

4.2. Functionaris Gegevensbescherming

Voor onafhankelijk toezicht en controle op de kwaliteit van de uitvoering van het privacybeleid heeft het AB RK Dordrecht een FG aangesteld (artikel 37 AVG). Deze functie wordt gepositioneerd binnen de RK Dordrecht. De FG heeft een onafhankelijke positie binnen de RK Dordrecht. De werkzaamheden die een FG uitvoert, hebben een wettelijke grondslag. Hij treedt op als adviseur voor de RK Dordrecht. De FG heeft, na formeel verzoek, het recht op toegang tot alle informatie en systemen en processen binnen de RK Dordrecht waarin privacygegevens een rol (kunnen) spelen. De FG geniet ontslagbescherming en doet zijn werk vrij van last en opdracht.

De FG heeft met het AB RK Dordrecht een privacy-GAP-analyse ontwikkeld. De FG houdt toezicht op het uitvoeren van de werkzaamheden die volgen uit de GAP-analyse en voert daarnaast zelfstandig controles uit. Zo controleert de FG of de registers op orde zijn. Ook in geval van datalekken moeten de procedures goed werken en dient de RK Dordrecht in control te zijn. Het is de FG die toeziet op de prioritering van de werkzaamheden door het AB RK Dordrecht en de wijze van implementatie van maatregelen.

Het Secretariaat RK Dordrecht informeert de FG over de uitvoering van onderzoeken waarbij persoonsgegevens worden gebruikt en informeert de FG onverwijld over datalekken. Ook afwijkingen op het privacybeleid die plaats kunnen vinden in de uitvoering van de wettelijke taken van de RK Dordrecht worden direct gerapporteerd.

De AVG verplicht tot het bijhouden van registers. Deze taken behoren ook toe aan het Secretariaat RK Dordrecht. Het Secretariaat RK Dordrecht beheert de volgende verplichte registers:

- Register van verwerkingsactiviteiten, met aantekeningen van DPIA's;
- Register van verwerkersovereenkomsten;
- Register van datalekken;
- Register voor aanvragen van betrokkenen.



5. Bijlage 1. Verantwoordelijkheid Wie & Hoe

Verantwoordelijkheid	Wie & Hoe
Afhandeling AVG-verzoeken betrokkenen op basis van privacybeleid RK Dordrecht	Het secretariaat is verantwoordelijk voor correcte en jegens betrokkenen transparante afwikkeling van AVG-verzoeken van betrokkenen. Het secretariaat rapporteert hierover aan de FG en registreert het verzoek en afhandeling in het hiervoor bestemde register. De FG ondersteunt het secretariaat hierin.
Awareness	De FG stelt samen met het AB RK Dordrecht vast welke training leden en medewerkers van de RK Dordrecht volgen en behoudt toezicht op het privacybewustzijn.
Verwerkersovereenkomsten	Daar waar verwerkingen uitbesteed worden aan derden, is het AB RK Dordrecht verantwoordelijk voor het sluiten van verwerkersovereenkomsten. Het secretariaat registreert de verwerkers en verwerkersovereenkomsten in het hiervoor bestemde register en rapporteert hierover aan de FG.
Beheer Privacybeleid RK Dordrecht	Het AB RK Dordrecht beheert het beleid. De FG rapporteert aan het AB RK Dordrecht over de voortgang en de kwaliteit van de uitvoering van het beleid door de Rekenkamer Dordrecht, en doet aanbevelingen voor verdere optimalisering. Waarborg voor optimalisering is het hanteren van de PDCA-cyclus via de GAP-analyse.
Toezicht op de naleving	De FG rapporteert ieder jaar aan het AB RK Dordrecht over geconstateerde privacyrisico's en de opvolging van de bevindingen uit de GAP-analyse. Het DB RK Dordrecht levert de FG de hiervoor benodigde informatie uit de desbetreffende privacyregisters aan.
GAP analyse	De FG ziet er samen met het AB RK Dordrecht op toe dat de bevindingen uit de GAP-analyse opvolging krijgen. Een plan hiertoe wordt jaarlijks opgesteld dat de basis is van de PDCA-cyclus.
Risico gedreven aanpak	Vertrekpunt voor het uitvoeren van onderzoeken van de RK Dordrecht is de uitvoering van een quickscan DPIA, DPIA Light of volledige DPIA. Na advies van de FG worden de privacy- (voor betrokkenen) en bestuurlijke risico's in kaart gebracht. De risico's worden door praktische, organisatorische en technische maatregelen beheerst.
Toezicht	De RK Dordrecht heeft een FG aangesteld (artikelen 37 t/m 39 AVG). De FG rapporteert aan het AB RK Dordrecht en onderhoudt de contacten met de AP. De FG is verantwoordelijk voor de controle op de naleving van het Privacybeleid RK Dordrecht.



Vaststellen Privacybeleid RK Dordrecht	Het AB RK Dordrecht stelt het beleid vast en bevordert de beschikbaarheid van voldoende middelen om privacy bescherming passend te waarborgen.
DPIA's	Het Secretariaat RK Dordrecht (laat) voert in voorkomend geval een DPIA uit(voeren) voor onderzoeken met een hoog privacyrisico. De FG voorziet elke uitgevoerde DPIA van advies en controleert de uitgevoerde maatregelen.

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

Functie	Taak
AB RK Dordrecht	<ul style="list-style-type: none"> • Vaststellen privacybeleid; • Naleving privacybeleid; • Minimaal 2 keer per jaar wordt de AVG-naleving door de RK Dordrecht op haar vergaderagenda geplaatst; • Opvolgen van werkzaamheden die volgen uit GAP analyse; • Aanstellen van FG; • Middelen beschikbaar stellen aan FG; • Sluiten van verwerkersovereenkomsten; • Besluitneming (Awb-besluit) op verzoeken op basis van AVG-rechten.
FG	<ul style="list-style-type: none"> • Houdt toezicht op het privacybeleid van de RK Dordrecht en monitort de opvolging van de bevindingen op basis van de GAP-analyse en voert daarnaast zelf controles uit; • Monitoren van relevante privacyontwikkelingen, bijvoorbeeld in wet- en regelgeving; • Awareness creëren bij het AB RK Dordrecht; • Ontwikkelen van templates t.b.v. het DB RK Dordrecht; • Adviseert over het uitvoeren van DPIA's en houdt toezicht op de uitvoering van de daarin gestelde maatregelen; • Adviseert het DB RK Dordrecht hoe te handelen bij datalekken; • Draagt zorg voor jaarlijkse verantwoordingsrapportages aan het AB RK Dordrecht; • Adviseert bij het sluiten van verwerkersovereenkomsten door de RK Dordrecht; • Meldt datalekken bij AP.
Secretariaat RK Dordrecht	<ul style="list-style-type: none"> • Dagelijkse uitvoering van het beleid binnen de RK Dordrecht; • In een vroeg stadium betrekken van de FG bij alle aangelegenheden die verband houden met de verwerking van persoonsgegevens door de RK Dordrecht; • (Laten) uitvoeren van Quickscan DPIA, DPIA Light of volledige DPIA voor onderzoeken waarin persoonsgegevens worden gebruikt (verantwoordingsplicht);



- Wint advies in bij de FG, als er een DPIA moet worden uitgevoerd;
- Wint, indien nodig, advies in bij de FG en de CISO van de gemeente Dordrecht over de naleving van het Informatiebeveiligingsbeleid van Gemeente Dordrecht en bij de inschakeling van onderzoeksbureaus;
- In behandeling nemen en correct afhandelen van AVG-verzoeken;
- Volgen van awareness training t.b.v. het vergroten van het privacy bewustzijn én optimalisering van de zelfredzaamheid op het gebied van AVG-naleving;
- Verstrekken van benodigde informatie aan de FG t.b.v. rapportages;
- Eerste aanspreekpunt voor de voorzitter van het AB RK Dordrecht betreffende naleving van de AVG;
- Voorbereiding en eventueel opstellen van verwerkersovereenkomsten;
- Mede beoordelen van externe communicatie over privacy en het bewaken van gezamenlijke belangen;
- Melding van datalekken bij FG.