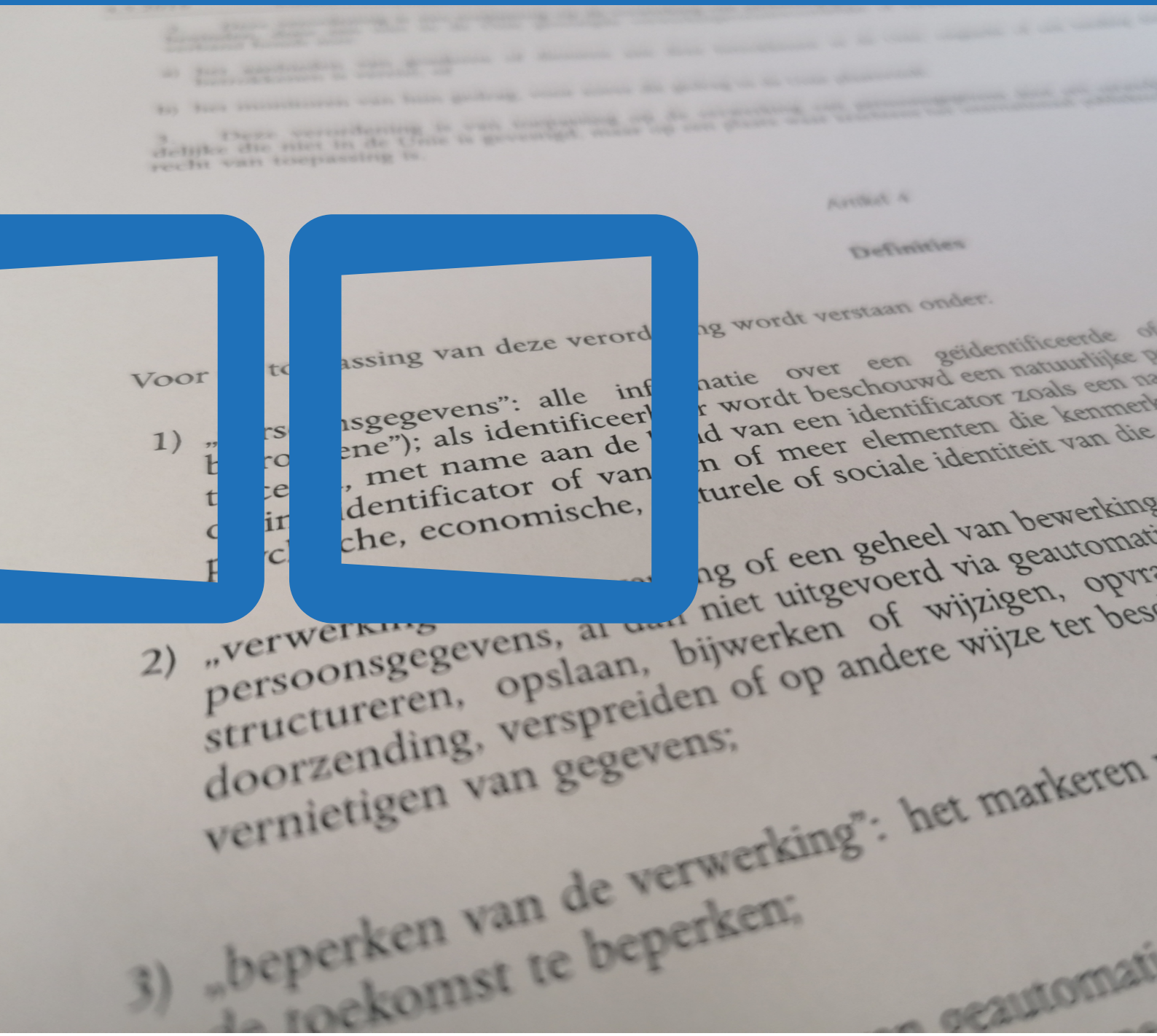
privacybeleid

Rekenkamer Rotterdam



vastgesteld 22 juli 2024

Rekenkamer
ROTTERDAM

Rekenkamer ROTTERDAM

inhoudsopgave

Rekenkamer ROTTERDAM

1 inleiding

1-1 doel privacybeleid

De Rekenkamer Rotterdam doet als onderzoeksinstituut onderzoek naar het gevoerde beleid in Rotterdam, Albrandswaard, Barendrecht, Capelle aan den IJssel, Krimpen aan den IJssel en Lansingerland. Bij het uitvoeren van deze onderzoeken worden persoonsgegevens verwerkt van onder meer ambtenaren en burgers (zie paragraaf 1-3 voor een definitie van 'persoonsgegevens'). Ook bij taken die horen bij de bedrijfsvoering van de rekenkamer, zoals inkoop en persoonsbeleid, worden persoonsgegevens verwerkt. Voor de rekenkamer is een goede en zorgvuldige omgang van persoonsgegevens van groot belang. In dit privacybeleid is beschreven hoe de rekenkamer omgaat met privacy en de bescherming van deze persoonsgegevens.

Dit beleid geldt als kader voor alle regels en afspraken met betrekking tot privacy en persoonsgegevens binnen de rekenkamer. Daarnaast is het beleid bedoeld als handboek voor de medewerkers van de rekenkamer.

Voor de toepassing van het privacybeleid maakt de Rekenkamer Rotterdam zoveel mogelijk gebruik van standaarden, modellen en handreikingen zoals die door de NVRR ten behoeve van lokale rekenkamers zijn opgesteld. Zo is in Bijlage A onze Privacyverklaring conform het voorbeeldformat van de NVRR opgenomen. Daarnaast is dankbaar gebruik gemaakt van documenten van andere rekenkamers, in het bijzonder van de Randstedelijke Rekenkamer.

1-2 de kern van de AVG

De AVG is een Europese verordening die ook wel bekend is onder de naam General Data Protection Regulation (GDPR). De AVG is van kracht sinds 25 mei 2018 en ziet toe op de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens zonder het vrije verkeer van persoonsgegevens te beperken. De AVG is van toepassing op de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en dus niet door een natuurlijk persoon in het kader van een louter persoonlijke of huishoudelijke activiteit.

De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht. Deze bescherming brengt extra verantwoordelijkheden mee voor bedrijven en overheden. De bescherming is technologieneutraal (niet afhankelijk van gebruikte technologieën) en dient te gelden bij zowel geautomatiseerde verwerking als handmatige verwerking van persoonsgegevens.

beginselen

In de AVG (artikel 5) staan zeven beginselen centraal waaraan elke verwerking van persoonsgegevens moet voldoen. Dit zijn de volgende beginselen:[1]

1 **rechtmatigheid, behoorlijkheid en transparantie**
Persoonsgegevens alleen mogen worden verwerkt voor gerechtvaardigde doeleinden (zie voorwaarden voor verwerking). De verwerking dient daarnaast netjes en verantwoord gebeuren. Ten slotte moet duidelijk zijn voor welke doelen persoonsgegevens worden verwerkt en hoe dat gebeurt.

2 **doelbinding**
Persoonsgegevens mogen alleen worden verzameld en verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Een nieuw doel moet verenigbaar zijn met het oorspronkelijke verzameldoel.

3 **minimale gegevensverwerking**
Er mogen gelet op het doel, niet te veel, maar ook niet te weinig gegevens worden verwerkt voor het doel. Er mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk voor het doel. Als er te weinig gegevens worden verwerkt, dan kan er ten onrechte een onvolledig beeld ontstaan van de betrokkene.

4 **juistheid**
De verwerkingsverantwoordelijke moet alle redelijke maatregelen nemen om ervoor te zorgen dat de gegevens correct en actueel zijn. Gegevens die dat niet (meer) zijn, moeten worden gewist of gecorrigeerd.

5 **opslagbeperking**
Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk voor het doel van de verwerking. Wanneer de gegevens niet langer noodzakelijk zijn, dan moeten zij worden vernietigd of gewist.

6 **integriteit en vertrouwelijkheid**
Persoonsgegevens moeten worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

7 **verantwoordingsplicht**
Organisaties hebben een verantwoordingsplicht, wat inhoudt dat ze moeten aantonen dat ze zich aan andere de zes beginselen van de AVG houden. Daarvoor gebruikt de Rekenkamer Rotterdam onder meer dit privacybeleid, de privacyverklaring en een verwerkingsregister.

voorwaarden voor verwerking

De verwerkingsverantwoordelijke mag persoonsgegevens verwerken als de verwerking is gebaseerd op een van de zes rechtsgrondslagen uit de AVG. Het gaat om de volgende zes grondslagen:

a de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;

b de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;

c de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

d de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;

1 Ministerie van Justitie en Veiligheid, Handleiding Algemene verordening gegevensbescherming, 8 januari, 2018, p. 22.

e verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

rechten betrokkenen
De AVG regelt dat betrokkenen verschillende mogelijkheden hebben om voor zichzelf op te komen bij de verwerking van hun gegevens. In de AVG staat bijvoorbeeld een speciaal artikel over toestemming. Hierin staat wat de voorwaarden zijn voor organisaties om geldige toestemming te krijgen van mensen om hun persoonsgegevens te verwerken. Zo moeten organisaties kunnen bewijzen dat zij geldige toestemming hebben gekregen. En moet het voor mensen net zo makkelijk zijn om hun toestemming in te trekken als om die te geven. De rechten van betrokken zijn verder toegelicht in hoofdstuk 8 van dit privacybeleid.

1-3 definities

Enkele belangrijke begrippen die in het privacybeleid gebruikt worden zijn hieronder gedefinieerd.

tabel 1-1: definities

begrip	omschrijving
betrokkenen	natuurlijke personen op wie de gegevens betrekking hebben
persoonsgegevens	Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke levende persoon. Een gegeven is een persoonsgegeven als het ervoor zorgt dat een persoon direct of indirect identificeerbaar is.
bijzondere persoonsgegevens	persoonsgegevens over iemands godsdienst of levensovertuiging, afkomst, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. Het is verboden om bijzondere persoonsgegevens te verwerken, tenzij er een wettelijke uitzondering is.
verwerkingsverantwoordelijke	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
verwerker	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, in opdracht van de verwerker, is een sub-verwerker.

1-4 leeswijzer

Na dit inleidende hoofdstuk over de AVG staat in hoofdstuk 2 beschreven wat de bevoegdheid van de rekenkamer is als het gaat om verwerken van persoonsgegevens. In hoofdstuk 3 staan de rollen en taken van de functionaris gegevensbescherming en privacy officer beschreven. Vervolgens komen het Data Protection Impact Assesement (hoofdstuk 4), hoe om te gaan met datalekken (hoofdstuk 5), het verwerkingsregister (hoofdstuk 6) en de verwerkersovereenkomsten (hoofdstuk 7) aan bod. Het voorlaatste hoofdstuk gaat in op de rechten van betrokkenen (hoofdstuk 8). In hoofdstuk 9 staat tenslotte hoe om te gaan met personeelsgegevens van de rekenkamermedewerkers.

Rekenkamer ROTTERDAM

2 bevoegdheid rekenkamer

2-1 bevoegdheid rekenkamer

In de Gemeentewet zijn de bevoegdheden van de rekenkamer verankerd. Hierbij wordt niet expliciet ingegaan op persoonsgegevens, maar uit de wet volgt wel dat de persoonsgegevens die door het gemeentebestuur worden verwerkt, ook door de rekenkamer mogen worden verwerkt. Zo bepaalt de Gemeentewet, artikel 183, lid 1, dat de rekenkamer bevoegd is 'alle documenten die berusten bij het gemeentebestuur te onderzoeken voor zover zij dat ter vervulling van haar taak nodig acht'. Dit betekent dat de rekenkamer (documenten die) persoonsgegevens (bevatten), bij de gemeente kan opvragen. Het gemeentebestuur is op zijn beurt, conform Gemeentewet artikel 183 lid 2, verplicht alle inlichtingen die de rekenkamer ter vervulling van haar taak nodig acht te verstrekken, waaronder dus ook persoonsgegevens die het gemeentebestuur heeft verzameld.

Uitzondering zijn bijzondere persoonsgegevens. Het gemeentebestuur is wel verplicht deze te leveren, maar de rekenkamer mag deze op grond van artikel 9 van de AVG niet zonder meer ontvangen. Bijzondere persoonsgegevens verwerken is namelijk verboden, tenzij er wordt voldaan aan één van de uitzonderingen in artikel 9 lid 2 van de AVG. De uitzonderingsgrond waar de rekenkamer het meest gebruik van maakt, is toestemming. Net als bij andere persoonsgegevens geldt bij bijzondere persoonsgegevens dat er voldaan moet worden aan de beginselen voor verwerking en dat er een duidelijke grondslag moet zijn (zie 1-2).

De Rekenkamer Rotterdam bepaalt in veel gevallen zelf het doel en de middelen van de verwerkingen van persoonsgegevens en is daarom verwerkingsverantwoordelijke in de zin van de AVG.

2-2 verwerking persoonsgegevens gemeente

Afspraken over onder welke voorwaarden de gemeente persoonsgegevens aan de rekenkamer verstrekt en over hoe de rekenkamer deze verwerkt zijn vastgelegd in het 'protocol verwerking persoonsgegevens Rekenkamer Rotterdam – gemeente Rotterdam' (zie website). Toezicht op een rechtmatige verwerking van de persoonsgegevens door de rekenkamer kan uitsluitend door de Functionaris Gegevensbescherming (hoofdstuk 3) plaatsvinden.

2-3 beveiligingsmaatregelen

De rekenkamer neemt passende maatregelen om misbruik, verlies, onbevoegde toegang en andere ongewenste handelingen met openbaarmaking van persoonsgegevens tegen te gaan. Persoonsgegevens worden bijvoorbeeld opgeslagen op locaties die enkel toegankelijk zijn voor het onderzoeksteam en indien nodig de directeur of de ondersteunende staf. Een ander voorbeeld is dat de rekenkamer persoonsgegevens ontvangt van de gemeente via een beveiligde omgeving. De

rekenkamer werkt de beveiligingsmaatregelen uit in haar informatiebeveiligingsbeleid.

Rekenkamer ROTTERDAM

3 functionaris gegevensbescherming en privacy officer

3-1 inleiding

Zowel een verwerker van persoonsgegevens als de verwerkingsverantwoordelijke dienen een functionaris voor gegevensbescherming (FG) aan te wijzen als er sprake is van verwerkingen verricht door een overheidsorgaan of overheidsinstantie (artikel 37 lid 1 AVG). Aangezien rekenkamers overheidsorganen zijn moet ook de Rekenkamer Rotterdam een FG aan wijzen. De regels over aanwijzing van de FG, de positie van de FG en de taken van de FG staan in artikel 37 tot en met 39 van de AVG.

3-2 taken en functie-eisen FG

De FG houdt toezicht op de toepassing en naleving van de AVG. De FG is geen eindverantwoordelijke; de eindverantwoordelijkheid blijft bij de verwerkingsverantwoordelijke, de rekenkamer.

De functie van FG moet worden vervuld door een deskundig en onafhankelijk persoon. Onder deskundig wordt verstaan het hebben van grondige kennis van de wet- en regelgeving in het algemeen en met betrekking tot de taken, verantwoordelijkheden en bevoegdheden van de Rekenkamer Rotterdam in het bijzonder. Met onafhankelijk wordt bedoeld dat de FG geen instructies ontvangt van de rekenkamer met betrekking tot de uitvoering van deze taken.

De Autoriteit Persoonsgegevens geeft de volgende richtlijnen over de positie van de FG in de organisatie:

1 u moet de FG genoeg middelen ter beschikking stellen om zijn taken goed te vervullen.
2 u mag de FG geen instructies geven over het uitvoeren van de FG-taken; de FG voert zijn taken en verplichtingen onafhankelijk uit.
3 de FG mag naast zijn FG-taken eventueel andere taken of functies vervullen, maar er mag geen sprake zijn van belangenverstrengeling.
4 u bent verplicht de contactgegevens van uw FG openbaar te maken.

3-3 invulling binnen de Rekenkamer Rotterdam

Om de onafhankelijkheid te waarborgen werkt de rekenkamer met een externe functionaris gegevensbescherming van Vijverberg Advocaten & Adviseurs. De FG heeft dus geen dienstverband bij de Rekenkamer Rotterdam en/of één van de zes gemeenten waar de rekenkamer voor werkt. Met de FG is afgesproken dat op het moment dat hij werkzaamheden verricht voor de gemeente Rotterdam of een van de regiogemeenten op het gebied van privacy, Vijverberg Advocaten & Adviseurs met de Rekenkamer Rotterdam overlegt welke consequenties dit heeft voor zijn functie van FG voor de Rekenkamer Rotterdam. Mogelijk kan dan een eventueel conflict worden

opgelost door een andere privacyjurist (tijdelijk) in te zetten als FG voor de Rekenkamer Rotterdam.

De rekenkamer heeft afgesproken dat de volgende taken worden vervuld door de FG:
- het informeren en adviseren over de verplichtingen die voor uw organisatie voortvloeien uit de AVG;
- samenwerken met de interne privacy officer;
- samenwerken met de functionaris die verantwoordelijk is voor de technische (ICT) en organisatorische beveiliging van persoonsgegevens;
- het desgevraagd toetsen en adviseren in complexere aangelegenheden op het gebied van privacy;
- toezien op de naleving van de AVG en het beleid dat uw organisatie heeft vastgesteld op het gebied van het verwerken van persoonsgegevens;
- het bewustmaken van de medewerkers van de noodzaak zorgvuldig om te gaan met de verwerking van persoonsgegevens;
- het adviseren bij het uitvoeren van een Data Privacy Impact Assessment (DPIA) in geval van nieuwe verwerkingsactiviteiten met naar verwachting een hoog risico voor de betrokkenen;
- ondersteuning bij het beoordelen en melden van datalekken;
- samenwerken met de Autoriteit Persoonsgegevens (AP) en het optreden als contactpunt voor de AP;
- het zijn van aanspreekpunt voor betrokkenen.

De concrete inzet is afhankelijk van het aantal privacy-issues dat binnen de organisatie speelt. Er vindt iedere drie maanden een overleg plaats tussen de FG, de privacy officer en de directeur.

Op 28 maart 2023 is de heer mr. Arjo Buurma van Vijverberg Advocaten & Adviseurs bij de Autoriteit Persoonsgegevens aangemeld als FG van de Rekenkamer Rotterdam. Het toegekende FG-nummer is FG014870.
Zijn contactgegevens zijn:
t: 079 3631919
e: fg@rekenkamer.rotterdam.nl

3-4 privacy officer

Sinds 1 januari 2023 heeft de Rekenkamer Rotterdam een privacy officer (ook wel privacy functionaris genoemd). Taken van de privacy officer zijn:
- zorgen voor bewustwording en voorlichting over privacy;
- medewerkers van de Rekenkamer Rotterdam adviseren over privacy;
- opstellen privacybeleid en interne regelingen over privacy;
- onderzoeken privacyrisico's door middel van DPIA's in samenwerking met projectleiders en FG;
- in het verwerkingsregister bijhouden welke persoonsgegevens verwerkt worden;
- bijhouden register datalekken en het overzicht beveiligingsincidenten;
- optreden als contactpersoon van de Functionaris Gegevensbescherming.

4 Data Protection Impact Assessment

4-1 inleiding

Een Data Protection Impact Assessment (hierna: “DPIA”), ook wel een gegevensbeschermingseffectbeoordeling genoemd, is een beoordeling van de effecten van een voorgenomen verwerkingsactiviteit op de bescherming van persoonsgegevens en de rechten en vrijheden van betrokkenen. De DPIA is een instrument om van projecten waarbij persoonsgegevens worden verwerkt, de effecten van betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen. Op basis hiervan kunnen maatregelen worden getroffen om deze effecten voor de betrokkenen te voorkomen dan wel te verkleinen. Daarnaast laat het uitvoeren van een DPIA zien dat er wordt voldaan aan de vereisten van de AVG. De regels over DPIA’s staan in artikel 35 en 36 van de AVG.

4-2 gebruik DPIA’s door de Rekenkamer Rotterdam

Op basis van de pre-DPIA wordt inzichtelijk gemaakt of een DPIA nodig is. De rekenkamer voert een pre-DPIA uit als er sprake is van minstens één van de volgende situaties bij een nieuwe verwerking:

- verwerking van grote aantallen persoonsgegevens;
- verwerking van grote aantallen bijzondere persoonsgegevens;
- verwerking van persoonsgegevens van kwetsbare groepen.

De (pre-)DPIA wordt opgesteld door de privacy officer in samenwerking met de projectleider. De FG wordt bij alle DPIA’s, dus ook bij de pre-DPIA, gevraagd om advies.

Voor het uitvoeren van een pre-DPIA heeft de rekenkamer een sjabloon ontvangen van de FG (bijlage 2). Voor het uitvoeren van een DPIA maakt de rekenkamer gebruik van het raamwerk en de bijbehorende handleiding van NOREA (beroepsorganisatie van IT-auditors in Nederland).[2]

2 De handleiding te vinden op https://www.norea.nl/handreikingen.

Rekenkamer ROTTERDAM

5 datalekken en beveiligingsincidenten

5-1 wat is een datalek?

Een datalek is de inbreuk op de beveiliging van persoonsgegevens. Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke levende persoon. Persoonsgegevens kunnen direct of indirect identificeerbaar zijn.

Er zijn drie soorten inbreuken op de beveiliging van persoonsgegevens:

1 Inbreuk op de vertrouwelijkheid
Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
2 Inbreuk op de integriteit
Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
3 Inbreuk op de beschikbaarheid
Wanneer er sprake is van een onbedoeld verlies van toegang tot persoonsgegevens, of onbedoelde vernietiging van persoonsgegevens.[3]

Een datalek betreft alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking van persoonsgegevens. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen had getroffen of niet.

Niet alle beveiligingslekken of -incidenten zijn een datalek:

beveiligingslek:	Er is een zwakke plek in de beveiliging. Een laptop is bijvoorbeeld niet beveiligd met een wachtwoord.
beveiligingsincident:	Door het lek in de beveiliging doet zich een incident voor. Er is sprake van een inbreuk op de beveiliging. Als er geen persoonsgegevens bij betrokken zijn is een beveiligingsincident geen datalek. Voorbeeld: een onbevoegd persoon maakt gebruik van de onbeveiligde laptop.
datalek:	Een beveiligingslek heeft geleid tot een inbreuk op de beveiliging van persoonsgegevens. Voorbeeld: de onbevoegde persoon heeft toegang gehad tot de laptop en persoonsgegevens ingezien.

Een datalek is bijvoorbeeld:

- een kwijtgeraakte USB-stick waar zich persoonsgegevens op bevinden;
- een werklaptop of werktelefoon met persoonsgegevens is gestolen of kwijt;
- een vastgestelde inbraak door een hacker;

3 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken#wat-is-een-datalek-precies-7964

- verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden (aan of CC);
- een besmetting met ransomware en er kan geen bruikbare back-up teruggezet worden;
- het verstrekken van een wachtwoord aan een derde;
- papieren met persoonsgegevens belanden op straat;
- een kwetsbaarheid in een applicatie waardoor persoonsgegevens gelekt worden.

5-2 procedure bij datalek

Als iemand van de Rekenkamer Rotterdam een mogelijk beveiligingsincident of datalek constateert (of daarover twijfelt), dan wordt direct de onderstaande procedure datalekken gevolgd. De procedure bestaat uit de volgende stappen:

stappenplan

1 signaleren en intern melden

Medewerkers signaleren en melden incidenten met persoonsgegevens (mogelijk datalek) bij zowel de privacy officer als de directeur. Dit gebeurt direct na ontdekken van het mogelijke datalek. Een eventuele melding bij de Autoriteit Persoonsgegevens moet namelijk binnen 72 uur gedaan worden, ook in het weekend.

2 beoordelen en melden aan FG

De privacy officer beoordeelt of er sprake is van een datalek. De privacy officer informeert bij alle datalekken de functionaris gegevensbescherming. De FG kan door de privacy officer om advies worden gevraagd en de FG kan (on)gevraagd advies geven over het datalek. Ook als er twijfel is of er sprake is van een datalek, wordt de FG om advies gevraagd.

3 maatregelen treffen

Het incident mag niet groter worden dan het al is. De te nemen maatregelen verschillen per beveiligingsincident. De directeur geeft in overleg met de privacy officer opdracht tot maatregelen die noodzakelijk zijn om het datalek te beëindigen en/of het beveiligingsrisico te beperken.

4 melden bij gemeente, betrokkenen, AP

melden bij gemeente

Als er een inbreuk heeft plaatsgevonden in verband met de door de gemeente verstrekte persoonsgegevens, stelt de rekenkamer de gemeente binnen 24 uur van dit datalek op de hoogte, waarna de gemeente en de rekenkamer afspraken maken over de verdere afhandeling en eventuele melding hiervan aan de Autoriteit Persoonsgegevens en/of de betrokkenen.

melden bij Autoriteit Persoonsgegevens

Datalekken moeten gemeld worden bij de Autoriteit Persoonsgegevens als:

- er gegevens van gevoelige aard zijn gelekt, zoals bijzondere persoonsgegevens (bijv. over gezondheid, godsdienst, afkomst, BSN), financiële of andere economische gegevens over iemand, gebruikersnamen, wachtwoorden en andere inloggegevens, kopieën van identiteitsbewijzen; of
- een grote hoeveelheid andere persoonsgegevens zijn gelekt.

Rekenkamer ROTTERDAM

Als de functionaris gegevensbescherming aangeeft dat het datalek gemeld moet worden bij de Autoriteit Persoonsgegevens dan moet dat via het webformulier dat te vinden is op de website van de AP, onverwijld, maar uiterlijk binnen 72 uur na constatering van het datalek worden gedaan.[4] Bij onzekerheid kan ook een pro forma melding worden gedaan, die later kan worden ingetrokken.

melden bij betrokkenen
Een datalek moet ook bij de persoon op wie de gelekte persoonsgegevens betrekking hebben (de werknemer, de sollicitant, de relatie, de geïnterviewde, etc) worden gemeld als:

- er gegevens van gevoelige aard zijn gelekt, zoals bijzondere persoonsgegevens (bijv. over de gezondheid van iemand, de godsdienst, de afkomst, het BSN), financiële of andere economische gegevens over iemand, gebruikersnamen, wachtwoorden en andere inloggegevens, kopieën van identiteitsbewijzen, gegevens over psychische of ander gezondheidsproblemen); en
- de gegevens niet op een juiste manier versleuteld zijn of er geen back-up voorhanden is; en
- er geen zwaarwegende redenen zijn om melding aan de betrokkene achterwege te laten (zoals een datalek van werknemersgegevens tijdens een nog geheim overnameproces).

Als hier sprake van is, dan moet de rekenkamer het datalek zo spoedig mogelijk melden bij de betrokkene. Dat kan door middel van een e-mail, brief of – als de omvang van het incident daarvoor aanleiding geeft – ook door een algemene kennisgeving in de media. In de melding moet de betrokkene ook geïnformeerd worden over de mogelijke maatregelen die de betrokkenen kan nemen om de negatieve gevolgen van het datalek te beperken.

De FG stelt vast of en bij wie het datalek moet worden gemeld. De rekenkamer volgt dit advies onverwijld op.

5 Vastlegging

Datalekken, de maatregelen die zijn getroffen en de interne correspondentie en de correspondentie met de externe functionaris gegevensbescherming worden door de privacy officer vastgelegd in het Logboek datalekken. Beveiligingsincidenten worden door de privacy officer vastgelegd in het Logboek beveiligingsincidenten.

6 Leren van beveiligingsincidenten en datalekken

Afhankelijk van het soort incident wordt het besproken in reguliere overleggen van het voltallige bureau, de onderzoeksstaf of team ondersteuning. Centrale vragen daarbij zijn:

- Wat kan er structureel verbeterd worden om dergelijke beveiligingsincidenten te voorkomen?
- Welke verdere maatregelen zijn noodzakelijk?

Lessen kunnen betrekking hebben op de informatiehuishouding, de algehele bedrijfsvoering, aanvullende beveiligingsmaatregelen, hoe toegang, autorisatie en verantwoordelijkheden zijn geregeld, authenticatieprocedures, de governance van de organisatie, werkprocessen en -routines, bewustwording, organisatiecultuur, enz.

4 Het webformulier is te vinden via: https://datalekken.autoriteitpersoonsgegevens.nl/.

Datalekken worden ook besproken in het reguliere overleg met de FG.

5-3 verantwoording in het jaarverslag

In het jaarverslag van de rekenkamer wordt verantwoord of en welke datalekken in het betreffende jaar hebben plaatsgevonden en welke maatregelen vervolgens zijn getroffen. Daartoe wordt het jaarverslag van de FG integraal opgenomen.

6 verwerkingsregister

6-1 inleiding

Om te voldoen aan de verantwoordingsplicht uit de AVG worden alle verwerkingsactiviteiten die de rekenkamer doet vastgelegd in een overzicht, namelijk het verwerkingsregister. Het verwerkingsregister is verplicht omdat de verwerking van persoonsgegevens door de rekenkamer niet incidenteel is en deels bestaat uit bijzondere persoonsgegevens.

6-2 invulling binnen de Rekenkamer Rotterdam

De Rekenkamer Metropool Amsterdam heeft de eerste opzet gemaakt van een model Verwerkingsregister en na overleg met de rekenkamers Rotterdam, Utrecht, Den Haag en de Randstedelijke Rekenkamer is dit als voorgesteld format aan de NVVR toegestuurd. De NVVR heeft dit model vastgesteld en naar haar leden gestuurd met het idee dat alle rekenkamers dit model kunnen toepassen. Het modelregister bestaat uit een deel voor onderzoeken en een deel voor bedrijfsvoering.[5]

De Rekenkamer Rotterdam past het model Verwerkingsregister van de NVRR toe. In het register staan alle onderzoeken die na het moment van invoering van de AVG (25 mei 2018) zijn gepubliceerd en waarvan de verwerking nog niet is afgerond. Onderzoeken waarbij enkel persoonsgegevens van contactpersonen ten behoeve van het onderzoek worden verwerkt, worden niet apart vermeld. Als er daarnaast nog andere persoonsgegevens worden verwerkt, bijvoorbeeld van burgers, dan wordt dit apart in het register vermeld. Zodra bij archivering de persoonsgegevens uit een onderzoek zijn vernietigd of gearchiveerd, is de verwerking afgerond en wordt het betreffende onderzoek uit het verwerkingsregister verwijderd.

Persoonsgegevens die verzameld worden in het kader van onderzoek worden 10 jaar bewaard en vervolgens vernietigd. Deze bewaartermijn is conform de selectielijst van de Vereniging van Nederlandse Gemeenten. Afwijken van de termijnen uit de VNG selectielijst is niet toegestaan.[6]

In het verwerkingsregister staan ook verwerkingen bij onderzoek gerelateerde activiteiten. Voorbeelden daarvan zijn contact met politici of evenementen of bijeenkomsten. De contactgegevens van algemene functionarissen (zoals wethouders, gemeentesecretarissen, griffiers, etc.) wordt bijgehouden door het secretariaat en alleen bij wijziging van functionarissen geschoond.

5 Het model is beschikbaar via: https://www.nvrr.nl/wiki/9151/model-register-van-verwerkingsactiviteiten-voor-rekenkamercommissies-2/.

6 In een eerdere versie van dit privacybeleid stond abusievelijk een termijn van 1 jaar vermeldt. Dit is in de versie van 22 juli 2024 gecorrigeerd.

6-3 actualisatie verwerkingsregister

Het verwerkingsregister wordt doorlopend geactualiseerd aan de hand van onderzoeksopzetten of eventuele tussentijdse wijzigingen in het verwerken van persoonsgegevens in onderzoeken. Het register wordt twee keer per jaar vastgesteld: in maart gelijktijdig met het jaarverslag en in september. De meest recent vastgestelde versie van het verwerkingenregister wordt gepubliceerd op de website van de rekenkamer (zie deze pagina).

7 verwerkersovereenkomsten

De rekenkamer sluit verwerkersovereenkomsten af met externe partijen die de opdracht krijgen om namens de verwerkingsverantwoordelijke (de Rekenkamer Rotterdam) persoonsgegevens te verwerken. Bijvoorbeeld voor het extern opslaan van persoonsgegevens in een cloud of hostingbedrijven van applicaties waarin persoonsgegevens worden verwerkt. De rekenkamer gebruikt daarvoor de standaard verwerkersovereenkomst gemeenten van de VNG.[7]

Als een organisatie of persoon weliswaar persoonsgegevens van haar klanten ziet, maar hij niet als primaire opdracht heeft om die persoonsgegevens te verwerken, dan kan worden volstaan met een geheimhoudingsverklaring. De standaardtekst voor de geheimhoudingsverklaring is opgenomen in bijlage 3.

Bij het aangaan van nieuwe overeenkomsten met externe partijen waarbij persoonsgegevens verwerkt worden, wordt de Functionaris Gegevensbescherming om advies gevraagd over de noodzaak een verwerkersovereenkomst af te sluiten. De privacy officer houdt een overzicht bij van de verwerkersovereenkomsten die zijn gesloten.

7 De meest actuele versie van deze overeenkomst en de bijbehorende handreiking is beschikbaar via de website van de VNG: https://www.informatiebeveiligingsdienst.nl/project/verwerkersovereenkomst-gemeenten/.

Rekenkamer ROTTERDAM

8 rechten betrokkenen

8-1 rechten van betrokkenen

Een betrokkene is een natuurlijke persoon op wie de gegevens betrekking hebben. Volgens de AVG hebben alle betrokkenen een achttal rechten. Hieronder staan deze rechten kort samengevat:

- **Recht op informatie** (artikel 13 en 14 AVG). Betrokkenen hebben bij het verkrijgen van persoonsgegvens recht op duidelijke informatie over wat er met hun persoonsgegevens gebeurt. Dit gaat onder meer om de contactgegevens van de verantwoordelijke en de FG, de verwerkingsdoeleinden en de rechtsgrond voor de verwerking.

- **Recht op inzage** (artikel 15 AVG). Betrokkenen hebben het recht om onder meer een kopie te ontvangen van de persoonsgegevens die van hen worden verwerkt. Bij een inzageverzoek moet ook informatie worden gegeven over de verwerking, zoals de verwerkingsdoeleinden en de rechten van betrokkenen.

- **Recht op rectificatie en aanvulling** (artikel 16 AVG). Het recht om de persoonsgegevens die worden verwerkt te laten wijzigen als de verwerking plaatsvindt op basis van onvolledige gegevens.

- **Recht op vergetelheid/gegevenswissing** (artikel 17 AVG). Betrokkenen hebben het recht om ‘vergeten’ te worden. In artikel 17 eerste lid AVG staat beschreven wanneer dit recht verkregen kan worden. Een voorbeeld is het intrekken van toestemming in combinatie met het ontbreken van een andere grond voor verwerking.

- **Recht op beperking van de verwerking** (artikel 18 AVG): Betrokkenen hebben op basis van een aantal gronden het recht om de verwerking van persoonsgegevens te beperken. Dat betekent dat persoonsgegevens dan niet mogen worden verwerkt (met uitzondering van de opslag van gegevens) of gewijzigd.

- **Recht op overdraagbaarheid/dataportabiliteit** (artikel 20 AVG). Het recht om persoonsgegevens over te laten dragen aan een andere partij. Dit recht geldt enkel als de verwerking gebeurt op basis van toestemming of een overeenkomst.

- **Recht op bezwaar** (artikel 21 AVG). Betrokken hebben het recht om bezwaar te maken tegen de gegevensverwerking. Als er bezwaar gemaakt wordt, dan staakt de verwerkingsverantwoordelijke de gegevensverwerking.

- **Recht met betrekking tot geautomatiseerde besluitvorming en profilering** (artikel 22 AVG). Betrokkenen hebben het recht om niet aan geautomatiseerde

besluitvorming te worden onderworpen. Dat betekent dat ze recht hebben op een menselijke blik bij besluiten.

Een uitgebreide beschrijving van deze rechten is te vinden in de AVG of op de website van de Autoriteit Persoonsgegevens.

8-2 onderdelen privacyverklaring

De Rekenkamer Rotterdam hanteert een *privacyverklaring* (zie bijlage 1). De privacyverklaring vat het privacybeleid in begrijpelijke taal samen. De privacyverklaring is opgesteld volgens het model van de NVRR.

In de privacyverklaring staan de volgende onderdelen:

1 algemeen
2 waarom wij uw persoonsgegevens verwerken
3 beveiliging
4 bewaartermijn
5 delen met anderen
6 uw rechten
7 cookiebeleid en -gebruik
8 aanvullende informatie over privacy
9 klachten
10 contactgegevens

De privacyverklaring is opgenomen in de bijlage van het privacybeleid en wordt ook apart gepubliceerd op de website van de rekenkamer.

8-3 interviewverslagen en correspondentie tijdens onderzoek

Voor de rekenkameronderzoeken voert de Rekenkamer Rotterdam veel interviews uit. De rekenkamer legt een interviewverslag altijd ter correctie en verificatie voor aan de geïnterviewde personen. In de onderzoeksrapporten kunnen passages uit interviews en inhoudelijke (e-mail)correspondentie over het onderzoek worden gebruikt die niet herleidbaar zijn tot een persoon en met daarbij een anonieme bronverwijzing zoals ‘interview ambtenaar’. De rekenkamer neemt geen namen en functies van ambtenaren of externen op in onderzoeksrapporten.

(Concept)interviewverslagen worden alleen gedeeld met de geïnterviewde(n) en niet met bijvoorbeeld leidinggevenden of de algemene contactpersoon van de gemeente voor de rekenkamer. Inhoudelijke e-mailcorrespondentie, conceptverslagen, de geaccordeerde verslagen en de correspondentie hierover worden bewaard op de netwerkschijf van de rekenkamer, die alleen toegankelijk is voor het onderzoeksteam. Daarmee geeft de rekenkamer invulling aan de eis uit het Kwaliteitshandvest G4+ dat het onderzoeksproces op basis van documenten in het dossier te reconstrueren is.

Rekenkamer ROTTERDAM

9 personeelsgegevens rekenkamermedewerkers

9-1 verwerking personeelsgegevens

De medewerkers van de Rekenkamer Rotterdam zijn in dienst van de gemeente Rotterdam. De gegevens voor de uitvoering van de arbeidsovereenkomst berusten bij de gemeente. Ook contactgegevens voor noodgevallen, verzuimregistratie en opleidingen zijn vastgelegd in de systemen van de gemeente Rotterdam. De directeur, de HR-adviseur en de directie-assistent hebben toegang tot deze gegevens.

De Rekenkamer Rotterdam verwerkt ook zelf persoonsgegevens van haar personeel. Deze verwerkingen staan opgenomen in het verwerkingsregister. Het gaat daarbij onder meer over de volgende persoonsgegevens en doelen:

- contactinformatie om contact te onderhouden;
- tijdsregistratie om te voldoen aan de arbeidstijdenwet;
- gegevens over ziekteverzuim t.b.v. externe arbodienst en bedrijfsarts;
- accountnamen en e-mailadressen voor gebruik van mobiele apparatuur, software en hardware;
- verjaardagen voor collegiale aandacht.

De Rekenkamer Rotterdam verwerkt de persoonsgegevens van personeel alleen voor bovenstaande doelen. Als er andere doelen zijn, dan worden werknemers vooraf geïnformeerd over de verwerking en het doel daarvan en krijgen zij de gelegenheid om bezwaar te maken. De bewaartermijnen van deze persoonsgegevens staan in het verwerkingsregister.

9-2 informatie op website en in rapporten

Zichtbaarheid is onderdeel van de uitvoering van de publieke taak van de rekenkamer. Daarom heeft de rekenkamer informatie over haar medewerkers op haar website staan. Doelen daarvan zijn arbeidsmarktcommunicatie, de organisatie een menselijk gezicht geven en een showcase voor expertise. Het gaat daarbij om naam, functie, persoonlijke introductie, foto, link naar een extern platform zoals bijvoorbeeld LinkedIn of ResearchGate. Alle medewerkers kunnen op ieder moment bezwaar maken voor vermelding van (een deel van) hun persoonsgegevens op de website op basis van artikel 21 AVG. Het is mogelijk om bezwaar te maken tegen de publicatie van een deel van deze gegevens, zoals wel de naam en geen foto. De persoonsgegevens worden dan zo snel mogelijk, maar in ieder geval binnen tien werkdagen, van de website verwijderd.

In de onderzoeksopzetten en onderzoeksrapporten staan de namen en de functies van het onderzoeksteam dat het onderzoek uitvoert. Ook hiervoor geldt dat medewerkers bezwaar kunnen maken tegen de publicatie van hun gegevens. Als medewerkers bezwaar maken, wordt hun naam niet opgenomen in de publicatie. Het is niet mogelijk om de met terugwerkende kracht bezwaar te maken, omdat

onderzoeksopzetten en onderzoeksrapporten openbaar zijn en aan de gemeenteraad zijn toegestuurd. De rekenkamer kan deze niet achteraf wijzigen.

9-3 rechten medewerkers

De rekenkamer informeert (nieuwe) medewerkers over het privacybeleid. Daarnaast kunnen medewerkers vragen over de verwerking van persoonsgegevens stellen aan de HR-adviseur, directeur of privacy officer. De rechten van betrokkenen (hoofdstuk 7) gelden ook voor het personeel. Medewerkers hebben de mogelijkheid om hun gegevens in te zien en eventueel te rectificeren, te beperken of te verwijderen. Bovendien hebben medewerkers te allen tijde het recht om een klacht over de verwerking van hun persoonsgegevens in te dienen bij de Autoriteit Persoonsgegevens.

Als de verwerking van persoonsgegevens is gebaseerd op toestemming, dan hebben medewerkers het recht om die toestemming in te trekken. Het intrekken van de toestemming doet geen afbreuk aan de rechtmatigheid van de verwerking van de persoonsgegevens voorafgaand aan de intrekking van de toestemming.

bijlagen

Rekenkamer ROTTERDAM

bijlage 1 privacyverklaring Rekenkamer Rotterdam

22 juli 2024

1 algemeen

De Rekenkamer Rotterdam, Albrandswaard, Barendrecht, Capelle aan den IJssel, Krimpen aan den IJssel en Lansingerland (hierna: 'rekenkamer') doet voor de gemeenteraden en de inwoners van deze gemeenten onafhankelijk onderzoek. De rekenkamer kijkt in haar onderzoeken naar het beleid en het handelen van de gemeente en geeft aanbevelingen voor verbeteringen. Om onze activiteiten goed te kunnen uitvoeren, is het soms nodig om uw persoonsgegevens te verwerken. De rekenkamer verwerkt uw persoonsgegevens op een zorgvuldige en veilige manier in overeenstemming met de Europese Algemene verordening gegevensbescherming (Avg) en de Uitvoeringswet Avg. Daarom beschrijft de rekenkamer graag waarom en hoe wij uw persoonsgegevens verwerken en hoe u uw rechten kunt uitoefenen.

2 waarom wij uw persoonsgegevens verwerken

2.1 onderzoeken

Voorafgaand aan elk onderzoek wegen wij zorgvuldig af welke persoonsgegevens nodig zijn voor het onderzoek, zodat wij dit met zo min mogelijk gegevens kunnen uitvoeren. In elke onderzoeksopzet wordt uiteengezet waarom en op welke wijze verwerking van persoonsgegevens nodig is.

Voor onze onderzoeken verwerken wij soms ook persoonsgegevens die wij bij de gemeente of bijvoorbeeld een gesubsidieerde instelling hebben opgevraagd. Zij zijn op grond van de Gemeentewet (artikel 183 lid 1) verplicht deze gegevens aan de rekenkamer te verstrekken en u daarover te informeren. Deze gegevens verwerken wij zonder u daarover nog afzonderlijk te informeren. De analyse van deze gegevens gebruiken wij in ons rapport. Uw persoonsgegevens zullen wij niet openbaar maken of met anderen delen.

Ook komt het voor dat wij u om persoonsgegevens vragen, bijvoorbeeld via een enquête, een interview of een groepsgesprek. Een enkele keer kunnen wij u vragen om bijzondere persoonsgegevens (zoals medische gegevens) als wij bijvoorbeeld een onderzoek doen in het sociaal domein. Ook kan het voorkomen dat wij u toestemming vragen om een (deel) van uw gemeentelijk dossier, waarin bijzondere persoonsgegevens staan, te mogen onderzoeken. De (bijzondere) persoonsgegevens verzamelen wij pas als u daarmee expliciet akkoord bent gegaan. U kunt deze toestemming op elk moment weer intrekken. Ook voor deze persoonsgegevens geldt dat wij deze niet openbaar maken.

2.2 onderzoek gerelateerde activiteiten

contact met politici

Van politici die verbonden zijn aan de gemeenten Rotterdam, Albrandswaard, Barendrecht, Capelle aan den IJssel, Krimpen aan den IJssel en Lansingerland registeren wij naast contactgegevens één bijzonder persoonsgegeven: de politieke

partij waar zij lid van zijn. Bij het benaderen van raadsleden of fracties voor bijvoorbeeld ons onderzoeksprogramma of onze onderzoeken nemen wij een zo groot mogelijke spreiding van politieke overtuiging in acht.

evenementen en bijeenkomsten
De rekenkamer organiseert soms evenementen en bijeenkomsten. Om personen te kunnen uitnodigen en welkom te heten, verwerken wij gegevens. Wij vragen u toestemming als wij uw gegevens willen hergebruiken voor toekomstige evenementen en bijeenkomsten van de rekenkamer.

contactgegevens
Als u zelf contact met ons opneemt verwerken wij de persoonsgegevens die u met ons deelt. Daarnaast biedt de rekenkamer inwoners van de gemeenten ook de mogelijkheid om hun ideeën te geven voor het onderzoeksprogramma. Wij vragen daarbij uw toestemming om uw gegevens te verwerken.

3 Beveiliging
De rekenkamer neemt de bescherming van uw persoonsgegevens serieus en heeft daarom passende maatregelen genomen om misbruik, verlies, onbevoegde toegang en andere ongewenste handelingen met openbaarmaking van persoonsgegevens tegen te gaan. Zo verloopt het verkrijgen van uw gegevens van de gemeente via een beveiligde omgeving. Uw gegevens worden door ons digitaal in een beveiligde map opgeslagen. Alleen de leden van het onderzoeksteam en indien nodig de directeur hebben hier toegang toe.

4 Bewaartermijn
De rekenkamer bewaart de verzamelde persoonsgegevens niet langer dan strikt nodig is, of wettelijk verplicht is, om de doelen te realiseren waar uw gegevens voor zijn verzameld.

4.1 Bewaartermijn onderzoeken
We beperken de verwerking van persoonsgegevens zoveel mogelijk. Daar waar mogelijk anonimiseren wij persoonsgegevens al tijdens het onderzoek. De rekenkamer is verplicht bepaalde gegevens te bewaren. Deze verplichting volgt uit de archiefwet en de daarop gebaseerde selectielijst voor archivering van de Vereniging voor Nederlandse Gemeenten (VNG).

Voor alle informatie die we voor onderzoeken verwerken geldt dat we deze tot tien jaar na afronding van een onderzoek moeten bewaren. Dat geldt dus ook voor persoonsgegevens die we tijdens het onderzoek hebben gebruikt. Voorbeelden zijn de verslagen van interviews en de resultaten van enquêtes. Na de termijn van tien jaar worden de gegevens vernietigd. (In een eerdere versie van de privacyverklaring stond een onjuiste termijn van 1 jaar.)

4.2 Bewaartermijn bij onderzoek gerelateerde activiteiten
Persoonsgegevens van politici bewaren wij zolang zij lid zijn van de gemeenteraad of raadscommissie. Binnen drie maanden na het beëindigen van hun lidmaatschap verwijderen wij de gegevens.

Na een evenement of bijeenkomst verwijderen wij de persoonsgegevens van de deelnemers, tenzij expliciet is aangegeven dat wij de gegevens mogen hergebruiken.

Als we nog andere activiteiten ondernemen waarbij persoonsgegevens verwerkt worden, dan worden die niet langer bewaard dan noodzakelijk voor het doel waarvoor ze zijn verzameld.

5 Delen met anderen

De rekenkamer verstrekt uw gegevens niet aan derden, tenzij dit nodig is voor de uitvoering van een afspraak met u of om te voldoen aan een wettelijke verplichting. Met organisaties die uw gegevens verwerken in opdracht van ons (bijvoorbeeld een enquêtebureau) sluiten wij een verwerkersovereenkomst om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens. De rekenkamer blijft verantwoordelijk voor deze verwerkingen.

6 Uw rechten

U heeft een aantal rechten waardoor u het gebruik van uw persoonsgegevens door de rekenkamer kunt controleren. U heeft recht om uw gegevens in te zien, te laten corrigeren en in bepaalde gevallen ook te laten verwijdering. Als u gebruik wilt maken van deze rechten dan kunt u een afspraak maken om bij de rekenkamer (zie 10. contactgegevens) langs te komen. Het is belangrijk dat u zich kunt legitimeren en kunt aantonen dat de gegevens die u wilt inzien, corrigeren of verwijderen daadwerkelijk van u zijn. Het is niet toegestaan om gegevens van andere personen in te zien.

U kunt een verzoek tot inzage, correctie of verwijdering ook op afstand doen, door uw verzoek te sturen naar info@rekenkamer.rotterdam.nl of *Rekenkamer Rotterdam, Meent 94, 3011 JP ROTTERDAM* ter attentie van de privacy officer. Ter verificatie dat het verzoek van u afkomstig is, vragen wij u een kopie van uw identiteitsbewijs bij het verzoek te voegen. Ter bescherming van uw privacy verzoeken wij u om op deze kopie uw pasfoto en Burgerservicenummer (BSN) zwart te maken. Als uw identiteit is gecontroleerd en deze controle is vastgelegd, wordt de kopie van uw identiteitsbewijs vernietigd. De rekenkamer zal zo snel mogelijk, maar uiterlijk binnen vier weken, op uw verzoek reageren.

7 Cookiebeleid en -gebruik

De rekenkamer heeft een website rekenkamer.rotterdam.nl. Op deze website maakt de rekenkamer gebruik van cookies. Een cookie is een klein tekstbestand dat bij het eerste bezoek aan deze website wordt opgeslagen op uw computer, tablet of smartphone. De cookies die wij gebruiken, zijn noodzakelijk voor de technische werking van de website en uw gebruiksgemak. Ze zorgen ervoor dat de website naar behoren werkt en onthouden bijvoorbeeld uw voorkeursinstellingen. Ook kunnen wij hiermee onze website optimaliseren.

Zodra u de website bezoekt kunt u kiezen welke cookies u wilt accepteren. Voor een goede werking van de website verwerken wij ook IP-adressen. Een IP-adres kan een persoonsgegeven zijn. De logbestanden met IP-adressen blijven een maand bewaard en worden daarna vernietigd. Wij maken gebruik van Google Analytics en combineren die dienst niet met andere Google-diensten. Wij hebben een verwerkersovereenkomst met Google gesloten en afgesproken dat Google de verzamelde persoonsgegevens niet voor eigen doeleinden mag gebruiken.

Rekenkamer ROTTERDAM

8 aanvullende informatie over privacy

Aanvullende informatie over hoe wij met persoonsgegevens binnen de rekenkamer omgaan kunt u vinden in ons privacybeleid. Een overzicht van alle verwerkingen van persoonsgegevens binnen de rekenkamer kunt u vinden in het register van verwerkingen.

9 klachten

Natuurlijk helpen wij u graag verder als u klachten heeft over de verwerking van uw persoonsgegevens. Hoe u een klacht kunt indienen en hoe wij deze afhandelen leest u in onze klachtenregeling.

Mocht u er desondanks toch niet samen met ons uitkomen, dan heeft u op grond van de privacywetgeving ook het recht om een klacht in te dienen bij de privacy toezichthouder, de Autoriteit Persoonsgegevens.

10 contactgegevens

Als u vragen heeft over deze privacyverklaring, neem dan contact op met onze externe functionaris gegevensbescherming via fg@rekenkamer.rotterdam.nl. Als u rechtstreeks de rekenkamer wilt benaderen dan kan dat via info@rekenkamer.rotterdam.nl of 010-2672242.

bijlage 2 sjabloon pre-DPIA

Vragen ter voorbereiding DPIA.

onderdeel A. beschrijving verwerking
A.1. Beschrijf in het kort wat de nieuwe gegevensverwerking (proces/wijziging/project/initiatief) inhoudt. Waarom wil de organisatie deze verwerking gaan uitvoeren? Wat is de scope van deze Pre-DPIA?
A.2. Wie is als proceseigenaar verantwoordelijk voor de privacy compliance van de verwerking? Wie is eindverantwoordelijk voor deze verwerking? Vermeld de namen en functies.
A.3. Geef aan van welke categorie(ën) van betrokkenen persoonsgegevens worden verwerkt. Geef daarbij aan wat de relatie is tot de betrokkenen.
O : Cliënten
O : Leerlingen
O : Patiënten
O : Medewerkers
O : Overigen
A.4 Geef aan welke categorieën van persoonsgegevens worden verwerkt.
O: Gewone persoonsgegevens, te weten:
O: Persoonsgegevens van kwetsbare groepen, te weten:
O: Bijzondere persoonsgegevens, te weten:
O: Strafrechtelijke persoonsgegevens, te weten:
A.5. Wat is de herkomst van de persoonsgegevens?
A.6. Aan welke categorieën ontvangers worden de persoonsgegevens verstrekt? Zijn deze als verwerker te kwalificeren?
A.7 In welke landen vindt de verwerking plaats? Worden persoonsgegevens aan derde landen (= landen buiten de EER) of aan internationale organisaties doorgegeven? Zo ja, zijn er passende waarborgen, en zo ja, welke zijn dat?
A.8. Bepaal welke bewaartermijnen voor deze persoonsgegevens van toepassing zijn.
A.9. Beschrijf de doel(en) van verwerking (meerdere antwoorden mogelijk).

A.10. Beschrijf de rechtsgrond(en) van verwerking (meerdere antwoorden mogelijk). (zie artikel 6 AVG)		
NB 1) Indien vraag 9 en/of 10 niet beantwoord kan/kunnen worden, is de verwerking waarschijnlijk niet toegestaan. *NB 2) Indien je organisatie deze verwerking gaat uitvoeren en zij een verwerkingsregister moet bijhouden, dan bevatten de antwoorden van vraag 1 t/m 10 de input om dit register voor deze verwerking op te stellen of aan te vullen.*		
onderdeel B. Analyse of er sprake is van een hoog privacyrisico, zodat een DPIA verplicht is		
B.1. Is een van de drie criteria van artikel 35 lid 3 AVG van toepassing? Zo ja, welke en licht dit toe.	nee	ja
B.2. Is/zijn er een of meerdere categorieën van de lijst van de Autoriteit Persoonsgegevens van toepassing? (https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667) Zo ja, welke en licht dit toe.	nee	ja
B.3. Is er anderszins sprake van een dusdanig hoog privacyrisico dat een DPIA nodig is? Bijvoorbeeld door gebruik van nieuwe technologieën (in combinatie met andere criteria).	nee	ja
conclusie B.4. Volstaat deze Pre-DPIA of is een DPIA verplicht? Geef op basis van de antwoorden van B.1 tot en met B.3 een eindoordeel of een DPIA verplicht is en licht toe.		
Wanneer de conclusie uit de stappen A. en B. is dat een ***DPIA verplicht*** *is, ga dan verder naar het Keuzehulpmodel waarmee je kunt bepalen of er een compacte of een uitgebreide DPIA nodig is en of je een verwerker moet betrekken bij het uitvoeren van de DPIA.* *Wanneer de conclusie uit de stappen A. en B. is dat een* ***DPIA niet verplicht*** *is, ga dan verder met* ***onderdeel C*** *en de ondertekening van de Pre-DPIA.*		
onderdeel C. Vaststellen beheersmaatregelen		
C.1. Vaststellen beheersmaatregelen indien geen DPIA nodig. Stel op basis van de analyse uit A. en B. per risico de benodigde beheersmaatregelen op en licht toe.		

Risico: Beheersmaatregel: Risico: Beheersmaatregel:		
C.2. Uitvoering Pre-DPIA, ondertekening proceseigenaar/directie en oordeel FG		
Betreft	Door (naam, functie, datum)	Eventuele opmerkingen
De Pre-DPIA is ingevuld door:		
De goedkeuring voor de te treffen beheersmaatregelen is verleend door:		
De resterende risico's zijn geaccepteerd door:		
De betrokken FG die heeft geadviseerd is:		
Samenvatting van het FG-advies:		
Acceptatie/verwerping van het FG-advies door:		
De Pre-DPIA blijft onder review en beheer van:		
Datum waarop de Pre-DPIA uiterlijk moet worden herzien:		
Goedkeuring Pre-DPIA door proceseigenaar/directie:		

Rekenkamer ROTTERDAM

bijlage 3 tekst geheimhoudingsverklaring

GEHEIMHOUDINGSVERKLARING
Ondergetekende

Naam en voornamen:
Geboren: _____-_____-_____ te _____
Functie/hoedanigheid:

verklaart door ondertekening van deze verklaring dat volledig en naar eer en geweten te zullen voldoen aan de van toepassing zijnde algemene in artikel 2:5 van de Algemene wet bestuursrecht neergelegde geheimhoudingsverplichting, welke bepaling luidt als volgt:

1 Eenieder die is betrokken bij de uitvoering van de taak van een bestuursorgaan en daarbij de beschikking krijgt over gegevens waarvan hij/zij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, en voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van die gegevens, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht of uit zijn taak de noodzaak tot mededeling voortvloeit.
2 Het eerste lid is mede van toepassing op instellingen en daartoe behorende of daarvoor werkzame personen die door een bestuursorgaan worden betrokken bij de uitvoering van zijn taak, en op instellingen en daartoe behorende of daarvoor werkzame personen die een bij of krachtens de wet toegekende taak uitoefenen.

Ondergetekende verklaart tevens ermee bekend te zijn aansprakelijk te zijn voor door overtreding van die verplichting aan de Rekenkamer Rotterdam en/of de gemeente Rotterdam veroorzaakte schade.

Ten slotte verklaart ondergetekende bekend te zijn met het bepaalde in artikel 272 Wetboek van Strafrecht, welke bepaling luidt als volgt:

1 Zij die enig geheim waarvan zij weet of redelijkerwijs moet vermoeden dat zij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.
2 Indien dit misdrijf tegen een bepaald persoon gepleegd is, wordt het slechts vervolgd op diens klacht.

Plaats en datum:

Handtekening:

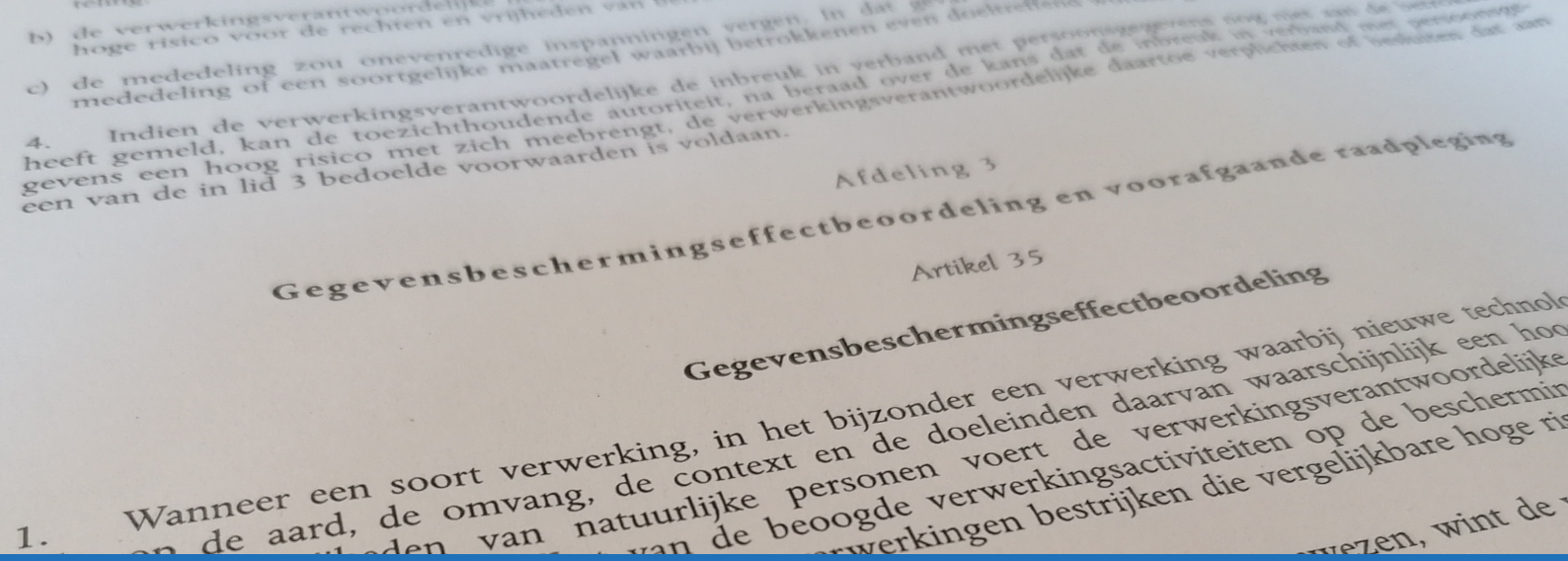
de rekenkamer
De gemeenteraad van Rotterdam heeft in december 1997 de Rekenkamer Rotterdam ingesteld. Sinds 14 juni 2021 is mevrouw prof.dr.ir. Marjolein van Asselt directeur. Zij is door de gemeenteraad voor zes jaar benoemd en beëdigd.

doel
De rekenkamer onderzoekt de doelmatigheid, doeltreffendheid en rechtmatigheid van het beleid, het financieel beheer en de organisatie van het gemeentebestuur. Zij doet dat ten behoeve van de gemeenteraad. Met interdisciplinair onderzoek en beleidsevaluatie draagt de rekenkamer bij aan het versterken van de lokale democratie en de kwaliteit van het gemeentebestuur.

onafhankelijk
De rekenkamer is net als de gemeentelijke Ombudsman onafhankelijk. Haar taken en bevoegdheden staan in de Gemeentewet en de verordening Rekenkamer Rotterdam. De rekenkamer bepaalt zelf waar ze onderzoek naar doet en heeft vergaande bevoegdheden om informatie te verzamelen. De raad en/of het college van B en W kunnen de rekenkamer wel vragen om onderzoek te doen. De rekenkamer stuurt hen jaarlijks haar onderzoeksplan en jaarverslag toe.

openbaar
Het onderzoek resulteert in openbare rapporten die de rekenkamer ter behandeling aan de raad aanbiedt. Zij bevatten tevens de reacties van de onderzochte organen en instellingen op de conceptrapporten (ambtelijk en bestuurlijk wederhoor). De rapporten worden toegelicht in (commissies van) de gemeenteraad.

voor Rotterdam en regio
Vijf regiogemeenten hebben zich in de loop der jaren aangesloten bij de Rekenkamer Rotterdam, namelijk Albrandswaard, Barendrecht, Capelle aan den IJssel, Krimpen aan den IJssel en Lansingerland.



Rekenkamer Rotterdam
Postbus 70012
3000 KP Rotterdam

telefoon
010 . 267 22 42

info@rekenkamer.rotterdam.nl
www.rekenkamer.rotterdam.nl

basisontwerp
dewerf•com, Zuid-Beijerland

fotografie
Rekenkamer Rotterdam

uitgave
Rekenkamer Rotterdam
juli 2024