# Privacyreglement

## Rekenkamercommissie ’s-Hertogenbosch

16 MEI 2018

# 1. Algemeen

In dit reglement laat de Rekenkamercommissie ’s-Hertogenbosch zien op welke manier zij dagelijks omgaat met persoonsgegevens en privacy, en wat er wettelijk wel en niet verantwoord is.

Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda. Ook lokale rekenkamers hebben de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Zo zijn ze verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Bijvoorbeeld in het kader van het rekenkameronderzoek of in contacten met burgers. Het beschermen van de privacy is complex, en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en nieuwe Europese wetgeving. Daarom vinden wij het belangrijk om transparant te zijn over de manier waarop wij als Rekenkamercommissie met persoonsgegevens omgaan, en de privacy waarborgen.

# 2. Onze aanpak

De Rekenkamercommissie ‘s-Hertogenbosch respecteert en beschermt de privacy en persoonsgegevens van de burgers. In de uitoefening van haar publiekrechtelijke taak houdt zij zich aan de wet en zoekt waar mogelijk de ruimte om de privacybelangen van zowel de burger als de doelstellingen van de Rekenkamercommissie naar beste inzicht te behartigen.

Als Rekenkamercommissie ’s-Hertogenbosch vinden wij het belangrijk dat onze leden, onderzoekers en secretaris privacybewust zijn. Dit verkleint de kans op onjuist gebruik van gegevens, lekken en nadelige gevolgen zoals boetes en negatieve publiciteit. Daarnaast tonen we hiermee aan dat wij als Rekenkamercommissie beschikken over leden, onderzoekers en secretaris die bewust zijn van de risico’s bij het werken met persoonsgegevens. Om privacybewust te worden en uiteindelijk ook te zijn, volgt de secretaris kennissessies en workshops op het gebied van privacy en omgaan met persoonsgegevens. Ook volgt de secretaris een e-learning waarmee naast kennisoverdracht ook de aanwezige privacy kennis wordt gemeten. Tevens stelt de gemeente ’s-Hertogenbosch ook voor de Rekenkamercommissie diverse handleidingen, factsheets en overige materialen ter beschikking om de leden, onderzoekers en secretaris hun werkzaamheden handvatten te bieden bij het verwerken van de persoonsgegevens waarmee zijwerken.

# 3. Wetgeving en definities

De Europese Verordening; de Algemene Verordening Gegevensbescherming (AVG) en de Nederlandse Uitvoeringswet AVG (UAVG) regelen het juridische kader voor de omgang met persoonsgegevens in Nederland. De AVG en UAVG zorgen onder andere voor versterking en uitbreiding van de privacyrechten met meer verantwoordelijkheden voor organisaties.

De volgende begrippen worden in de AVG gebruikt:

Betrokkene: De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt. Dit is niet alleen een burger, maar heeft bijvoorbeeld ook betrekking op een medewerker van de gemeente, of de contactpersoon van een organisatie waar de gemeente mee werkt.

Persoonsgegevens: Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon, een mens dus, zijn persoonsgegevens. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon. Denk hierbij aan naam, adres, woonplaats, geboortedatum of -plaats, e-mailadres, handtekening, telefoonnummer, inkomen of geslacht. Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren, strafrechtelijk verleden, godsdienst of het Burgerservicenummer (BSN). Deze gegevens mogen in principe niet worden verwerkt. Of alleen worden gebruikt bij uitdrukkelijke toestemming van de betrokkene, wanneer de gegevens door de betrokkene duidelijk openbaar zijn gemaakt of wanneer de wet het toestaat.

Data Protection Impact Assessment (DPIA): in het Nederlands 'gegevensbeschermingseffectbeoordeling' genoemd. Met een DDPIA worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy.

Verantwoordelijke: Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerker: De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

Verwerking: Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

Overige wetgeving om in het bijzonder rekening mee te houden:

*Wet openbaarheid van bestuur (Wob):* Via de Wob (en straks wellicht de Wet Open Overheid) kun je een verzoek om informatie indienen bij de gemeente. Bij het verzoek bekijkt de Rekenkamercommissie altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

*Wet hergebruik van overheidsinformatie*: De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de Rekenkamercommissie altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

# 4. Reikwijdte

Het privacyreglement is van toepassing op alle verwerkingen van persoonsgegevens door de Rekenkamercommissie. Oftewel: voor alle verwerkingen die door en binnen de Rekenkamercommissie plaatsvinden. Dit privacyreglement vormt een praktische handleiding en verdere uitwerking van de wettelijke regelgevingen. Het geeft de regels en uitgangspunten voor de eerlijke, zorgvuldige en rechtmatige verwerking van persoonsgegevens. Op die manier kan hiermee een nog betere verwerking van persoonsgegevens plaatsvinden door en binnen de Rekenkamercommissie.

# 5. Verantwoordelijke voor de verwerking

De Rekenkamercommissie is eindverantwoordelijkheid voor de verwerkingen van persoonsgegevens die door leden, onderzoekers en secretaris van de Rekenkamercommissie worden uitgevoerd.

# 6. Verwerkingen

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. Wij verzamelen en verwerken als Rekenkamercommissie persoonsgegevens, omdat wij onderzoek verrichten, ook bij burgers, instellingen en bedrijven. Het gaat bijvoorbeeld om onderzoek binnen het sociaal domein.

Onder verwerken worden in ieder geval de volgende handelingen begrepen:

1. Verzamelen, vastleggen en ordenen
2. Bewaren, bijwerken en wijzigen
3. Opvragen, raadplegen, gebruiken
4. Verstrekken door middel van doorzending
5. Verspreiding of enige andere vorm van ter beschikkingstellen
6. Samenbrengen, met elkaar in verband brengen
7. Afschermen, uitwissen of vernietigen van gegevens

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

# 7. Doeleinden

Algemeen uitgangspunt is dat persoonsgegevens alleen verzameld worden als daarvoor een doel bestaat. Dit doel moet welbepaald, duidelijk omschreven en gerechtvaardigd zijn. Ook moet steeds nagaan worden of het verwerken van persoonsgegevens noodzakelijk is voor het doel. De verwerkingsdoelen zijn het ‘waarom’ van het verwerken van persoonsgegevens. Doelen zijn van belang voor verschillende normen. Denk hierbij aan onder andere het bepalen wie verantwoordelijk is voor de verwerking van persoonsgegevens. Of de vraag of het delen van deze gegevens met andere organisaties is toegestaan. Ook zijn doelen van belang voor het

vaststellen van bewaartermijnen en het informeren van de burger. Zo weet je hoe lang het nodig is om de persoonsgegevens te bewaren of waar je burgers over moet informeren.

Daar waar over verwerking van persoonsgegevens in bijzondere wetgeving (zoals WMO en Participatiewet) niets is geregeld, gelden de strenge regels van de AVG (en de daarmee samenhangende Uitvoeringswet AVG).

Een belangrijke eis is dat doelen vooraf specifiek geformuleerd en bepaald moeten zijn. De doelen mogen dus niet te ruim en vaag omschreven zijn of achteraf bepaald worden. Verwerking voor een ander doel dan het oorspronkelijke doel is alleen onder strikte voorwaarden toegestaan. Zo zal er een directe relatie moeten zijn met het doel waarvoor de persoonsgegevens eerder zijn verzameld. Ook moet men rekening houden met de soort gegevens. Algemeen geldt: hoe gevoeliger het gegeven, hoe minder snel er sprake is van verenigbaar gebruik en de gegevens niet verder mogen worden verwerkt. Dus niet mogen worden gebruikt voor een ander doel dan waarvoor deze eerder zijn verzameld. Ook moet men rekening houden met de gevolgen van de beoogde verwerking voor de betrokkene. Denk hierbij aan het vooraf inlichten van de burger over het doel waarvoor de gegevens worden gebruikt als de burger zijn persoonsgegevens aan de Rekenkamercommissie geeft. Bijvoorbeeld voor een interview of een enquête.

# 8. Rechtmatige grondslag

De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dit betekent dat we als Rekenkamercommissie moeten verantwoorden op basis waarvan we persoonsgegevens van bijvoorbeeld een burger verwerken. Een uitzondering hierop is het hiervoor besproken geval waarin persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze zijn verzameld. Dit is onder strikte voorwaarden toegestaan. Een goed voorbeeld hiervan is het verder gebruiken van de gegevens voor wetenschappelijk onderzoek en statistiek.

Iedere verwerking van persoonsgegevens moet kunnen worden gebaseerd op één van de volgende zes grondslagen:

1. de betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend;
2. de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, waarbij ook rekening moet worden gehouden met de onderhandelingsfase;
3. de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de Rekenkamercommissie onderworpen is;
4. de gegevensverwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene(in het kader van leven of dood, bijvoorbeeld delen van gegevens bij opname spoedeisende hulp);

5. de gegevensverwerking is noodzakelijk voor de uitoefening van een taak van algemeen belang door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
6. de gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de Rekenkamercommissie of van een derde aan wie de gegevens worden verstrekt. Maar als het belang op bescherming van zijn privacy voor de betrokkene zwaarder weegt, dan is het verwerken van gegevens op grond van een gerechtvaardigd belang niet van toepassing.

Voor alle grondslagen zal er altijd een noodzaak moeten zijn om die gegevens te verwerken. Of het verwerken van bepaalde gegevens noodzakelijk is, moet altijd gemotiveerd worden.

Van de zes grondslagen zijn voor de Rekenkamercommissie in de praktijk de wettelijke grondslag en de goede vervulling van een publiekrechtelijke taak leidend.

# 9. Wijze van verwerking

De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt. In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.

Persoonsgegevens moeten dus juist, ter zake dienend, up-to-date en niet bovenmatig veel zijn in het licht van het doel van de verwerking. Dit betekent dat alleen die persoonsgegevens mogen worden gebruikt die strikt noodzakelijk zijn voor het doel van de verwerking. Wanneer het bijvoorbeeld voldoende is om iemands contactgegevens te gebruiken, is het niet nodig om ook een pasfoto en BSN te vragen. Sowieso gelden voor het gebruik van het BSN strenge regels. Wanneer ook met anonieme gegevens volstaan kan worden, mogen geen herleidbare persoonsgegevens gebruikt worden.

### 9.1 Organisatorische maatregelen

Niet alleen zorgt de Rekenkamercommissie ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht. Ook is het van belang dat de personen die daadwerkelijk werken met deze gegevens weten wat hun verantwoordelijkheid is. En hoe ze zorgvuldig om moeten gaan met persoonsgegevens. Het is dus belangrijk dat de leden, onderzoekers en secretaris van de Rekenkamercommissie zich bewust zijn van de regels en gedragsnormen rondom privacy. Deze organisatorische maatregelen dragen ook bij aan een bewustwording binnen de Rekenkamercommissie. De medewerkers moeten zich bewust zijn

van het belang van privacy. Zo moeten zij persoonsgegevens verwerken zoals is bepaald in het privacyreglement.

### 9.2 Beveiliging

Daarnaast beveiligt de Rekenkamercommissie alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevenskunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Als uitgangspunt geldt dat naarmate de risico’s van de verwerking hoger liggen er betere beveiligingsmaatregelen moeten worden getroffen. De gemeente heeft hiervoor een specifiek beleid opgesteld in de vorm van het Informatiebeveiligingsbeleid, dat ook geld voor de Rekenkamercommissie. Het is aan de gemeente en de Rekenkamercommissie om te bepalen hoe de persoonsgegevens organisatorisch en technisch moeten worden beveiligd. Hoe de gemeente dit doet staat in het informatiebeveiligingsbeleid van de gemeente en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

Middels steekproeven wordt gecontroleerd of het gebruik van de systemen en de verwerking van persoonsgegevens in lijn is met de wet- en regelgevingen dit privacyreglement. Ook voor overige systemen wordt gebruik gemaakt van het loggen van gegevens. Indien daar aanleiding toe is, zal ook hier worden gecontroleerd of de systemen en verwerking van persoonsgegevens worden gebruikt conform de wet- en regelgevingen dit privacyreglement.

## 10. Doorgifte aan derden

Persoonsgegevens mogen in principe niet worden doorgegeven naar een organisatie in een land buiten de EU. Dit komt omdat binnen de EU een goede bescherming voor de persoonsgegevens is, en daarbuiten niet in alle gevallen. Onder doorgifte wordt o.a. verstaan: het opslaan (bijvoorbeeld in de Cloud) of het ter beschikking stellen aan een organisatie buiten de EU. Hieronder valt niet het via internet zichtbaar maken van persoonsgegevens aan personen buiten de EU. De Rekenkamercommissie geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie.

## 11. Transparantie en communicatie

### 11.1 Informatieplicht

Betrokkenen moeten geïnformeerd worden over de verwerking van de eigen persoonsgegevens door de Rekenkamercommissie. Het moment van informeren en de manier waarop is afhankelijk van de vraag hoe de persoonsgegevens worden verzameld. Namelijk, zijn de gegevens rechtstreeks van de betrokkene verkregen of op een andere manier. In bepaalde gevallen verwerkt de Rekenkamercommissie persoonsgegevens op basis van een wettelijke verplichting en is zij niet verplicht om de betrokkene te informeren.

Als de persoonsgegevens door de burger of medewerker zelf worden aangeleverd, dan moet deze over de verwerking van zijn gegevens vooraf worden geïnformeerd. Als persoonsgegevens over de betrokkene niet direct bij deze persoon maar ergens anders, zoals een andere organisatie, dan hoeft de betrokkene pas op een later moment geïnformeerd te worden. De burger moet dan pas geïnformeerd worden als die persoonsgegevens door de Rekenkamercommissie worden vastgelegd. Of op het moment dat de gegevens voor het eerst aan een andere organisatie worden gegeven en dit uiteraard nodig is.

**11.2 Inzage**

Betrokkenen hebben recht op inzage in de eigen persoonsgegevens. De betrokkene hoeft geen reden op te geven voor zijn inzageverzoek, maar hij mag niet overdreven veel verzoeken in korte tijd indienen. Als een betrokkene vraagt om inzage, dan heeft hij of zij recht op een volledig overzicht van de gegevens die worden gebruikt. Ook moet inzage worden gegeven in de herkomst van de gegevens, de ontvangers van de gegevens en de doelen van de verwerking van de persoonsgegevens. De Rekenkamercommissie zorgt ervoor dat aan dit verzoek tijdig en volledig wordt voldaan.

**11.3 Correctie en verwijdering**

Naast een recht op inzage heeft de betrokkene ook recht op correctie, aanvullen, verwijderen of afschermen van de eigen persoonsgegevens. Aan dit verzoek moet alleen gehoor worden gegeven als de gegevens onjuist zijn of onvolledig zijn voor het doel waarvoor de gegevens worden verzameld. Dit verzoekmoet ook worden gerespecteerd als de gegevens niet relevant zijn of in strijd met de wet worden gebruikt.

De betrokkene moet in zijn verzoek duidelijk aangeven welke gegevens om welke reden moeten worden aangepast. Het recht kan niet worden gebruikt om meningen of onderzoeksresultaten te wijzigen. Als positief wordt besloten op het verzoek, dan moeten de wijzigingen zo snel mogelijk worden doorgevoerd.

De wijzigingen of verwijderingen van persoonsgegevens moeten ook worden doorgegeven aan andere organisaties aan wie de Rekenkamercommissie de gegevens heeft verstrekt. Deze afspraken zijn standaard op genomen in de verwerkersovereenkomsten van de Rekenkamercommissie.

**11.4 Bezwaar (nieuwe term onder de AVG)**

De betrokkene heeft de mogelijkheid om zich te verzetten tegen het gebruik van zijn persoonsgegevens. Als een betrokkene zich verzet tegen gebruik van de gegevens, dan mag de Rekenkamercommissie de gegevens niet meer gebruiken. Ook al is de gegevensverwerking op zich gerechtvaardigd en toegestaan. Er is een aantal situaties waar het recht van verzet kan worden ingezet. Allereerst in het geval er sprake is van bijzondere persoonlijke omstandigheden en de verwerking is gebaseerd op de publiekrechtelijke taak. Of in de situatie dat het een lid, onderzoeker of medewerker van de Rekenkamercommissie is en deze vanwege

bijzondere persoonlijke omstandigheden bezwaar maakt tegen de verwerking van zijn gegevens gebaseerd op een gerechtvaardigd belang. In beide situaties kan er niet met succes verzet worden ingediend tegen het opnemen van de persoonsgegevens in openbare registers die bij wet zijn ingesteld.

### 11.5 Indienen van verzoek

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden. De Rekenkamercommissie heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal de Rekenkamercommissie laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de Rekenkamercommissie, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de Rekenkamercommissie aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

## 12. Plichten van de Rekenkamercommissie

### 12.1 Register van verwerkingen

Vanaf 25 mei 2018 komen er voor de Rekenkamercommissie extra verplichtingen bij. Zo is de gemeente verplicht om te documenteren welke persoonsgegevens worden verwerkt, wat het doel ervan is, van wie of waar deze gegevens afkomstig zijn en met wie deze gegevens worden gedeeld. Daarnaast moeten we per verwerking documenteren en verantwoorden op basis van welke wettelijke grondslag de Rekenkamercommissie deze persoonsgegevens verwerkt.

### 12.2 Bewaartermijnen

De Rekenkamercommissie bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van haar taken, of zoals vastgelegd in de Archiefwet. In de AVG worden geen bewaartermijnengenoemd.

De hoofdregel is: bewaren mag zolang het nodig is voor het doel van de verwerking.

In een aantal wetten zijn specifieke bewaartermijnen opgenomen voor bepaalde persoonsgegevens. Als geen bewaartermijn aanwezig is dan moet goed kunnen worden onderbouwd waarom persoonsgegevens voor een bepaalde termijn worden bewaard. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Na afloop van de bewaartermijnen moeten de persoonsgegevens worden vernietigd of geanonimiseerd. Dit geldt niet alleen voor de gegevens zelf, maar ook voor kopieën en back-ups. Voor alle persoonsgegevens geldt dat de vernietiging onomkeerbaar moet zijn. Het gaat dus niet om het plaatsen van de bestanden in de prullenbak en de prullenbak legen, maar bijvoorbeeld om het overschrijven van data met nullen, enen en willekeurige karakters (data wiping).

### 12.3 Meldplicht datalekken

De meldplicht datalekken houdt in dat de Rekenkamercommissie zo snel mogelijk (binnen 72 uur) een melding doet bij de AP zodra een ernstig datalek zich heeft voorgedaan. Een datalek is een inbreuk op de beveiliging, die flinke nadelige gevolgen heeft voor de burger of voor de bescherming van de persoonsgegevens. Denk hierbij aan een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak op het netwerk (hack). Als de kans bestaat dat het datalek nadelige gevolgen zou kunnen hebben voor burgers, dan moet de Rekenkamercommissie het daarnaast óók melden bij de betrokken burgers. Daarnaast moet de burger worden geïnformeerd over welke maatregelen wij als Rekenkamercommissie nemen om de risico’s en schade te beperken.

Naast het melden moeten wij ook alle datalekken documenteren. Met deze documentatie moet de Autoriteit Persoonsgegevens kunnen controleren of wij als Rekenkamercommissie aan de meldplicht hebben voldaan.

### 12.4 Verwerkersovereenkomst

Verwerkersovereenkomsten moeten iedere keer worden afgesloten wanneer derden – ook wel verwerkers genoemd – in opdracht van de Rekenkamercommissie persoonsgegevens verwerken. Te denken valt aan een onderzoeksbureau dat voor ons (delen van) een onderzoek uitvoert. Uiteraard moeten er duidelijke afspraken worden gemaakt over hoe deze derde moet omgaan met de gegevens die zij van de Rekenkamercommissie c.q. de gemeente krijgt. Denk hierbij aan welke gegevens men nodig heeft om haar taak uit te oefenen, de manier waarop de organisatie de gegevens heeft beveiligd en wat zij moet doen als er een datalek is. De Rekenkamercommissie heeft een standaard verwerkersovereenkomst die in deze gevallen moet worden gebruikt.

### 12.5 De Privacy Impact Assessment (DPIA)

Met een DPIA worden de effecten en risico’s van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt. Rekenkamercommissie c.q. de gemeente ‘s-Hertogenbosch voert deze alleen uit wanneer:

1. er een (geautomatiseerde) verwerking plaatsvindt met een hoog risico;
2. er een (geautomatiseerde) verwerking plaatsvindt waarvan de Autoriteit Persoonsgegevens heeft aangegeven dat daarvoor een DPIA verplicht is;
3. een grootschalige verwerking plaatsvindt;
4. of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt.

### 12.6 Privacy by Design en privacy by default

Bij de aanschaf of ontwikkeling van producten, systemen of processen moet altijd rekening worden gehouden met de bescherming van persoonsgegevens. We noemen dit Privacy by Design (Pbd) en privacy by default. Voor alle producten, systemen of processen moeten de

technische en organisatorische maatregelen ervoor zorgen dat standaard allee die gegevens worden gebruikt die nodig zijn voor het doel. Als blijkt dat bij een systeem gevoelige of bijzondere persoonsgegevens worden verwerkt en dit mogelijk een hoog privacy risico met zich meebrengt, zijn we verplicht om een Privacy Impact Assessment(DPIA) uit te voeren.

**12.7 Functionaris voor de gegevensbescherming**

De gemeente heeft een functionaris voor de gegevensbescherming (FG) aangesteld. Deze functioneert tevens als FG voor de Rekenkamercommissie. Door het aanstellen van een FG wordt een belangrijke stap gezet in de manier waarop de Rekenkamercommissie aan haar burgers wil uitdragen dat zij serieus omgaat met de verwerking van persoonsgegevens. De aanwijzing van een FG wordt voor de gemeente onder de AVG verplicht. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de AP. De Rekenkamercommissie stelt ook een FG aan om daarmee het eigen toezicht en controle te organiseren. Hij heeft een belangrijke coördinerende rol en adviseert over oplossingen over privacy. De FG houdt vanuit een onafhankelijke positie intern toezicht op de manier waarop door de Rekenkamercommissie wordt omgegaan met persoonsgegevens. Belangrijk is ook dat hij aan de voorkant een rol speelt bij de inrichting van processen. En als laatste is de FG het formele aanspreekpunt is voor burgers als zij hun rechten als betrokkene willen uitoefenen. Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de gemeentelijke afdelingen overneemt. De afdelingen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens.

Voor vragen over privacy of over deze toelichting kunt u contact opnemen met de functionaris voorgegevensbescherming van de gemeente ’s-Hertogenbosch via: fg@s-hertogenbosch.nl

**12.8 Verantwoordelijkheid**

De Rekenkamercommissie is verantwoordelijk voor de wijze waarop zij persoonsgegevens verwerkt. De FG kan adviseren of oordelen dat een bepaalde gegevensverwerking niet conform het beleid en het reglement wordt uitgevoerd.

Als de aanwijzing(en) door de FG ten aanzien van de desbetreffende gegevensverwerking niet binnen een redelijke termijn wordt opgevolgd, wordt het volgende escalatiemodel gehanteerd:

1. Het Presidium van de gemeenteraad wordt geïnformeerd en de opvolging wordt zijn verantwoordelijkheid;

Bij het niet opvolgen van de aanwijzing wordt:

2. De gemeenteraad geïnformeerd en de opvolging wordt zijn verantwoordelijkheid;

**12. 9 Gouden regels van privacy & informatiebeveiliging**

Om als Rekenkamercommissie voor iedereen op een duidelijke en begrijpelijke wijze het belang van het zorgvuldig omgaan met persoonsgegevens te laten zien, heeft de gemeente ’s-Hertogenbosch 10 regels opgesteld, die wij onderschrijven. Deze bestaan uit 6 regels die specifiek zien op het werken met (en verwerken van) persoonsgegevens. De andere 4 regels zijn de regels die zien op de informatiebeveiliging, maar zijn ook van toepassing op het zorgvuldig omgaan met persoonsgegevens. Deze 10 regels worden gezamenlijk aangeduid als ‘de 10 gouden regels van privacy en informatiebeveiliging’. De 10 gouden regels zijn:

1. Behandel persoonsgegevens vertrouwelijk en integer
2. Verwerk niet meer persoonsgegevens dan nodig
3. Motiveer en leg vast wat je doet
4. Leg uit waarom we persoonsgegevens verwerken en wees transparant
5. Weet wanneer je persoonsgegevens mag delen met anderen
6. Ga zorgvuldig met persoonsgegevens om
7. Ga verantwoord om met wachtwoorden
8. Ken de risico's van e-mail, internet en sociale media
9. Ga verantwoord om met mobiele faciliteiten
10. Maak melding van beveiligingsincidenten

Dit reglement treedt in werking na vaststelling door de Rekenkamercommissie ’s-Hertogenbosch.