Aan: de leden van de NVRR
Datum: 12 april 2018
Betreft: Informatie over de Algemene Verordening Gegevensbescherming (AVG)

Geachte leden,

Op 25 mei 2018 is de Europese Algemene Verordening Gegevensbescherming (AVG) van toepassing. Naar verwachting zal in dezelfde periode ook de uitvoeringswet AVG in werking treden. De privacybescherming voor alle personen van wie u gegevens verwerkt, wordt hierdoor verbeterd. Voor u als rekenkamer(commissie)[1] betekent dit dat uw verantwoordelijkheid groter wordt. Het gaat bijvoorbeeld niet alleen om gegevens van burgers die u in het kader van onderzoek verzamelt, maar ook om gegevens van ambtenaren, raadsleden of geraadpleegde experts. Ook als u onderzoek uitbesteedt, blijft u verantwoordelijk. U moet kunnen aan tonen dat u zich aan de AVG en de uitvoeringswet houdt. Voldoet u daaraan niet, of kunt u dat niet aantonen, dan kan de Autoriteit Persoonsgegevens een (forse) boete opleggen.

In deze brief geeft de NVRR u algemene richtinggevende adviezen als ondersteuning aan uw taak de privacy van personen, waarvan u gegevens verwerkt, goed te beschermen en daarmee te voldoen aan de AVG en de uitvoeringswet. Naast deze adviezen zal de NVRR op korte termijn enkele algemene modellen ter beschikking stellen die in het kader van de AVG noodzakelijk of wenselijk worden geacht. Tot slot zal de NVRR een Q en A publiceren van algemene vragen die leven bij rekenkamers.

De AVG vraagt ook om maatwerk. Wat dit concreet voor uw rekenkamer(commissie) betekent is afhankelijk van de aard en omvang van de persoonsgegevens die u verwerkt. Wij raden u aan om dit af te stemmen met uw Functionaris Gegevensbescherming (FG). Zie hierna over de FG.

Adviezen
Wij adviseren u de volgende stappen te ondernemen zodat u klaar bent voor de AVG (en de uitvoeringswet):
1. Stel een Functionaris Gegevensbescherming aan

Doorloop de volgende stappen samen met uw Functionaris Gegevensbescherming:
2. Word bewust van de inhoud van de AVG en de uitvoeringswet
3. Breng in kaart welke (bijzondere) persoonsgegevens u verwerkt
4. Ga na of u een Data Protection Impact Assessment (DPIA) moet uitvoeren
5. Tref passende beveiligingsmaatregelen

[1] De AVG geldt voor alle overheids- en bestuursorganen. Deze brief is gericht aan alle decentrale rekenkamer(commissie)s, van gemeenten, provincies en waterschappen.

6. Weet hoe te handelen bij datalekken
7. Ga na of privacybeleid moet worden opgesteld
8. Stel een privacyverklaring op
9. Kom verwerkersovereenkomsten overeen
10. Zorg dat betrokkenen hun rechten kunnen uitoefenen

Tot slot, voer de regelhulp van de Autoriteit Persoonsgegevens uit om op hoofdlijnen in te schatten in hoeverre u al voldoet aan de AVG en bespreek dit met uw FG.

Hieronder gaan we nader in op de voorgaande stappen.

1. Stel op korte termijn een Functionaris Gegevensbescherming (FG) aan
Verwerkt uw rekenkamer(commissie) persoonsgegevens? Dan bent u, als overheidsorganisatie, verplicht een Functionaris Gegevensbescherming (FG) aan te stellen. Geef voor 25 mei 2018 aan de Autoriteit Persoonsgegevens door wie uw FG is. Gebruik hiervoor dit webformulier. U kunt kiezen uit de volgende varianten:

- U stelt de FG van uw gemeente[2] aan voor uw rekenkamer(commissie);
- U stelt zelf intern een FG aan of huurt een externe FG in;
- U stelt samen met anderen (bijvoorbeeld andere rekenkamercommissies) een FG aan of huurt gezamenlijk een externe FG in;

Een FG moet voldoen aan de richtlijnen voor functionarissen voor gegevensbescherming. Kiest u voor de FG van uw gemeente, dan zal deze waarschijnlijk voldoende deskundig en vaardig zijn. Een aandachtspunt is echter de onafhankelijkheid van de FG, eveneens een in de richtlijn gestelde eis. Het is niet uit te sluiten dat onafhankelijkheid van de FG van de gemeente niet is te waarborgen. Zo zou er in de toekomst een belangenconflict kunnen ontstaan, bijvoorbeeld als u onderzoek uitvoert naar de naleving van de AVG bij uw gemeente en u daarmee tevens het functioneren van de FG beoordeelt. Stelt u zelf (of samen met anderen) een FG aan, dan kunt u dit ondervangen. Houd echter wel de richtlijnen voor de aanstelling van de FG in acht. Een keuze voor de FG kan ook in de loop van de tijd worden veranderd. Voor de meeste rekenkamer(commissie)s zal het vanwege de tijdsdruk verstandig zijn om gebruik te maken van de FG van de gemeente. Mocht u voornemens zijn (op termijn) zelf een FG aan te stellen, dan kunt u bij de aanstelling van de FG van de gemeente al een termijn vaststellen waarbinnen u de taken onafhankelijk wenst onder te brengen (bijvoorbeeld 6 maanden of één jaar). De NVRR onderzoekt de mogelijkheid om rekenkamer(commissie)s te helpen bij het gezamenlijk aanstellen van FG's.

2. Word bewust van de inhoud van de AVG en uitvoeringswet
Het is van belang dat alle leden van de rekenkamer(commissie), uw personeel en de externe ondersteuning die u inhuurt, zich verdiepen in de Algemene Verordening Gegevensbescherming (AVG) en uitvoeringswet AVG. Een eerste stap daarbij is om kennis te nemen van de Handleiding Algemene verordening gegevensbescherming van het Ministerie van Justitie en Veiligheid. Zo worden alle leden en het personeel zich bewust van de rechten en de plichten die voortvloeien uit de AVG en de uitvoeringswet en kunnen zij proactief de AVG naleven. Aangezien het vereiste kennisniveau van de omgang met persoonsgegevens en de bewaking van de privacyrechten continue aandacht eisen, kunnen wij ons voorstellen dat u jaarlijks onderzoekt in hoeverre u voldoet aan de AVG en de uitvoeringswet. In uw jaarverslag kunt u over de conclusies en over de mogelijk te ondernemen acties rapporteren. Daarnaast

[2] Voor 'gemeente' kan ook provincie of waterschap worden gelezen

kan het zijn dat u uw werkwijzen moet veranderen en dat u deze wijzigingen verwerkt in uw kwaliteitshandvest, -handboek of –werkwijze.

3. Breng in kaart welke (bijzondere) persoonsgegevens u verwerkt
Breng in kaart welke (bijzondere) persoonsgegevens u verwerkt en met welk doel.[3] U kunt hiervoor een *verwerkingsregister* gebruiken. De VNG heeft een handreiking register van verwerkingen voor gemeenten ter beschikking gesteld die u voor dat doel kunt gebruiken.[4]
Ga van de persoonsgegevens die u verwerkt na:

- op basis van welke wettelijke grondslag u de gegevens mag verwerken. Grondslag voor het verwerken van persoonsgegevens zijn:
    - Het doen van onderzoek als de rekenkamer persoonsgegevens ontvangt van de gemeente of bijvoorbeeld gesubsidieerde instelling (artikel 182 Gemeentewet in samenhang met artikel 6 lid 1 onder e AVG -vervulling taak van algemeen belang).
    - Het doen van onderzoek als de rekenkamer persoonsgegevens rechtstreeks van de betrokkene ontvangt, zoals bij enquêtes (artikel 182 Gemeentewet in samenhang met artikel 6 lid 1 a AVG - expliciete toestemming).
- of u ook bijzondere persoonsgegevens mag verwerken. Bijzondere persoonsgegevens (o.a. geloof, ras, religieuze- of levensbeschouwelijke overtuigingen en gezondheid) mogen alleen onder strenge vooraarden worden verwerkt. Rekenkamer(commissie)s mogen bijzondere persoonsgegevens alleen verwerken als de betrokkene daar uitdrukkelijke toestemming voor heeft gegeven (artikel 9 lid 2 onder a AVG).
- of persoonsgegevens echt nodig zijn voor het doel van de verwerking (veelal onderzoek). Verwijder de overige -niet noodzakelijke- persoonsgegevens (de 'nice-to-haves').
- hoe lang gegevens bewaard moeten worden. Vernietig of anonimiseer deze zodra het kan.

4.*Ga na of u een Data protection impact assessment (DPIA) moet uitvoeren*
Ga na of u een Data protection impact assessment (DPIA) moet uitvoeren zodat u (vooraf) de privacyrisico's van een gegevensverwerking in kaart brengt en vervolgens maatregelen treft om de risico's te verkleinen. Op de website van de Autoriteit Persoonsgegevens zijn negen criteria weergegeven om af te wegen of een DPIA moet worden uitgevoerd. Er kunnen verschillende methoden gebruikt worden om een DPIA uit te voeren, één daarvan is de handreiking voor de uitvoering voor een DPIA. Deze vindt u op de website van de beroepsorganisatie van IT-auditors (NOREA). Ook andere methoden kunnen worden gebruikt. In bijlage 2 van het richtsnoer gegevensbeschermingseffectenbeoordelingen (DPIA) staan de criteria waaraan de gekozen methode moet voldoen.

[3] Persoonsgegevens zijn alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon. U kunt hier bijvoorbeeld denken aan NAW-gegevens, uitkeringsgegevens, maar ook aan ip-adressen. Bijzonder persoonsgegevens zijn persoonsgegevens die naar hun aard bezien extra gevoelig zijn: gegevens waaruit ras of etnische afkomst blijkt, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid en persoonsgegevens van strafrechtelijke aard. Van *verwerken* is sprake als u (bijzondere) persoonsgegevens verzamelt, vastlegt, opslaat, wijzigt, opvraagt, raadpleegt, gebruikt, verstrekt, wist of vernietigt.
[4] De NVRR zal dit model nog toespitsen voor gebruik door rekenkamer(commissie)s.

5. Tref passende beveiligingsmaatregelen
Het is van belang dat u passende beveiligingsmaatregelen treft om de beveiliging van de verwerking van persoonsgegevens te waarborgen. Wat passend is, hangt af van de gevoeligheid van de persoonsgegevens en de risico's die de aard van de verwerking met zich meebrengt voor de betrokkene. Veelal volstaat het naleven van het beveiligingsbeleid van uw gemeente. Maakt u geen of niet alleen gebruik van de faciliteiten van uw gemeente (bijvoorbeeld omdat u mails laat binnenkomen op een ander emailadres of op een eigen telefoon), stel dan in samenwerking met uw FG (aanvullend) beveiligingsbeleid op en leef dit na.

6. Weet hoe te handelen bij datalekken
Het belangrijkste is dat u weet hoe u datalekken kunt voorkomen. Verder is het belangrijk dat u weet hoe u moet handelen indien zich onverhoopt toch een datalek voordoet. Zo moet u datalekken documenteren, over het algemeen binnen 72 uur na ontdekking melden bij de Autoriteit Persoonsgegevens en onder bepaalde omstandigheden moet u ook de betrokkenen daarover informeren. Gezien de relatief korte tijd om te handelen is het van belang dat de taken goed vast liggen. Om aan te tonen dat u aan de AVG voldoet moet u beschikken over een actuele procedure datalekken. Stel samen met uw FG vast of u gebruik kunt maken van de procedure van uw gemeente of dat u zelf een procedure voor de omgang met datalekken moet opstellen. Zie voor nadere informatie de factsheet melden datalekken van de informatiebeveiligingsdienst

7. Ga na of privacybeleid moet worden opgesteld
Afhankelijk van de omvang en de aard van uw verwerkingen is het nodig om een privacybeleid (ook wel gegevensbeschermingsbeleid) op te stellen. Exacte criteria zijn niet te geven, maar als het aantal verwerkingen toeneemt, ze complexer worden of grotere gevolgen hebben voor de betrokkenen, doet u er verstandig aan om een privacybeleid op te stellen. In alle gevallen kan privacybeleid nuttig zijn. Het geeft u inzicht of u voldoende maatregelen heeft getroffen om persoonsgegevens te beschermen. Daarnaast is het een manier waarmee u als rekenkamer(commissie) aan uw doelgroep en de Autoriteit Persoonsgegevens laat zien hoe u omgaat met persoonsgegevens en privacy. De VNG heeft een model privacybeleid en -reglement voor gemeenten beschikbaar gesteld.[5]

8. Stel een privacyverklaring op
Verwerkt u persoonsgegevens, dan bent u verplicht de betrokkene daarover te informeren.[6] Dit kan met een privacyverklaring (ook wel privacy statement genoemd). De privacyverklaring is in ieder geval verplicht wanneer u via uw website persoonsgegevens verzamelt. De privacyverklaring kunt u op uw website plaatsen en meesturen met mails. De VNG heeft een handreiking privacyverklaring opgesteld. Binnenkort zal de NVRR een model privacyverklaring uitbrengen dat is toegesneden op rekenkamer(commissie)s.

[5] Het opstellen van een privacybeleid vergt maatwerk, waarbij inhoudelijk gebruik kan worden gemaakt van de privacyverklaring (zie stap 8).
[6] De NVRR kan zich voorstellen dat deze informatieplicht niet absoluut is indien persoonsgegevens tijdens het onderzoek zijn verkregen van de onderzochte (zoals gemeente / provincie / waterschap of gemeenschappelijke regeling). De NVRR heeft bij de Autoriteit Persoonsgegevens de vraag neergelegd in hoeverre de uitzonderingsgronden van de AVG van toepassing zijn (zie ook de paragraaf "NVRR – Antwoorden op algemene vragen" in deze brief).

9. Kom verwerkersovereenkomsten overeen
Als rekenkamer(commissie) bent en blijft u verantwoordelijk voor de verwerking van persoonsgegevens. Ook als u gebruik maakt van een derde, zoals een onderzoeksbureau, een bureau die voor u (elektronisch) enquêteert, maar ook wanneer u gebruik maakt van Google Analytics. Het is van belang en wettelijk verplicht dat u met deze verwerker afspraken maakt en deze afspraken in een overeenkomst vastlegt. Met een verwerkersovereenkomst sluit u uit dat de derde partij de persoonsgegevens voor eigen doelen mag verwerken. Bovendien krijgt u hiermee het recht om bijvoorbeeld een audit te (laten) doen op de verwerking en mag uw verwerker alleen met uw toestemming subverwerkers inschakelen. De VNG heeft een model voor een verwerkersovereenkomst opgesteld. Binnenkort zal de NVRR een model verwerkersovereenkomst uitbrengen dat is toegesneden op rekenkamer(commissies).

Gebruikt u op uw website Google Analytics, dan is het noodzakelijk om dit privacy vriendelijk in te stellen. In deze handleiding van de Autoriteit Persoonsgegevens leest u hoe.

10. Zorg dat betrokkenen hun rechten kunnen uitoefenen
Betrokkenen – personen waarover u persoonsgegevens verwerkt – hebben rechten. Zoals het recht om te weten dat u persoonsgegevens over hen verwerkt en met welk doel. Ook hebben zij het recht op inzage, correctie, verwijdering en beperking van persoonsgegevens. Ten slotte hebben betrokkenen het recht om een klacht in te dienen. Het ligt voor de hand dat ze dat eerst bij u doen, maar ze kunnen ook rechtstreeks bij de Autoriteit Persoonsgegevens een klacht indienen.

Betrokkenen kunt u actief informeren door een privacyverklaring op uw website te plaatsen en in uw correspondentie daar naar te verwijzen (zie stap 8). Daarnaast kunt u betrokkenen informeren wanneer u hen expliciet om toestemming vraagt om hun persoonsgegevens te mogen verwerken.

Vraagt een betrokkene inzage of verzoekt een betrokkene zijn of haar gegevens te verwijderen, dan bent u verplicht binnen een maand na dit verzoek een beslissing te nemen in de zin van de Algemene wet bestuursrecht en de betrokkene daarover te informeren. Tegen deze beslissing staat bezwaar en beroep open.[7]

Betrokkenen kunnen bij u klagen. Bij de afhandeling van deze klacht is naast de AVG en de uitvoeringswet ook hoofdstuk 9 van de Algemene wet bestuursrecht (klachtenbehandeling) van belang. Klaagt de betrokkene bij de Autoriteit Persoonsgegevens, dan zal deze contact met uw FG opnemen.

Om op een ordentelijke manier met de informatieplicht, verzoeken en klachten om te gaan raden wij u aan te bezien of u uw werkwijze of procedures moet aanpassen.

[7] Net zoals in de *Handreiking lokale rekenkamer en rekenkamerfunctie* van de NVRR (januari 2011, p. 52) wordt er in deze tekst vanuit gegaan dat een rekenkamercommissie ook een bestuursorgaan is in de zin van de Awb.

NVRR – modellen
Het is op grond van de AVG niet voldoende dat u maatregelen neemt om te waarborgen dat uw verwerkingen in overeenstemming met de AVG plaatsvinden, maar u moet dit ook kunnen aantonen. In verband met deze 'aantoonplicht' zal de NVRR enkele handreikingen en modellen van de VNG verder ontwikkelen, zodat ze meer zijn toegespitst op de praktijk van rekenkamer(commissie)s. Het betreft:

- Model verwerkingsregister (stap 3)
- Model privacyverklaring (stap 8)
- Model verwerkersovereenkomst (stap 9)

Zodra deze handreikingen en modellen beschikbaar komen zullen ze worden gepubliceerd op de website van de NVRR: www.nvrr.nl

NVRR – Antwoorden op algemene vragen
De AVG en de uitvoeringswet zijn nieuw. De NVRR heeft nog niet op alle vragen een antwoord. Wij geven drie voorbeelden. Wij vragen ons af of rekenkamer(commissie)s betrokkenen altijd moeten informeren of dat er ook uitzonderingen zijn waarvoor dat niet geldt, bijvoorbeeld bij grote databestanden die de rekenkamer van de gemeente ontvangt tijdens een onderzoek. Ook vragen wij ons af of een betrokkene altijd zijn of haar rechten moet kunnen uitoefenen, of dat het denkbaar is dat deze rechten beperkt worden als de rekenkamer de gegevensverwerking heeft ontvangen van de gemeente in het kader van de uitoefening van zijn taak.
Een derde voorbeeld, de archiefwet is van toepassing op de rekenkamer(commissie)s, maar welke persoonsgegevens moeten worden gearchiveerd en in hoeverre kan de openbaarheid daarvan worden beperkt? In de komende periode gaan wij deze vragen afstemmen met de Autoriteit Persoonsgegevens of andere deskundigen en zullen wij de antwoorden op die vragen publiceren op de website van de NVRR.