FG-advies

Aan: het gemeentebestuur
Van: de functionaris gegevensbescherming
Betreft: WPG-audit

Datum: 12 oktober 2022

Doel

U heeft momenteel te maken met de verplichte externe audit onder de Wet politiegegevens (WPG-audit). Ik heb gemerkt dat deze audits onnodig uitgebreid en met te weinig expertise worden uitgevoerd om er betekenis aan te kunnen hechten. Dat ligt niet aan de gemeente maar aan de landelijke aanpak. Het doel van deze notitie is om u een alternatief te bieden.

Uw opties

Optie 1 – Het alternatief treft u aan als auditplan volgens de bijlage. Kiest u voor deze optie, dan leeft u de EU-privacywetgeving na conform de bedoeling en in overeenstemming met het gemeentelijk beschermingsbeleid. U kunt rekenen op onderkenning hiervan in mijn jaarlijkse FG-verslagen. De gemeente bespaart zich de tijd, kosten, energie en het risico van onnodige discussie, die met de huidige WPG-audits gepaard gaan.

Wél een punt van attentie: met optie 1 wijkt u af van het auditonderdeel in de Nederlandse Wet politiegegevens en gerelateerde lagere regelingen. Ik zie dat echter als een formaliteitskwestie (zie het kompas op pagina 5). Materieel waarborgt u juist doelmatiger en doeltreffender de bescherming van persoonsgegevens. De Wet politiegegevens – de titel zegt het al – was ook nooit bedoeld voor gemeenten.

Optie 2 – houdt in dat u de Nederlandse auditregeling wél uitvoert. In dat geval dient u voor het einde van dit jaar een afschrift van het auditrapport naar de Autoriteit Persoonsgegevens te sturen. Paradoxaal genoeg moet ik als FG die handelswijze echter afkeuren. Het manco dat dan ontstaat, is dat u niet-passend auditbeleid voert dat conflicteert met de EU-privacywetgeving. Hoger recht gaat voor lager recht: niet alleen de Nederlandse wetgever maar ook de gemeente heeft zich aan de EU-normstelling te houden.

Indien gewenst, licht ik een en ander ook mondeling toe.

Sergej Katus

Mr. S.H. Katus
Functionaris Gegevensbescherming

Toelichting

Landelijk worden momenteel de externe audits uitgevoerd volgens de Wet politiegegevens en de Regeling periodieke audit politiegegevens (RPA). De eerste audits hadden eind 2021 moeten zijn afgerond met afschrift aan de Autoriteit Persoonsgegevens. De AP verleent echter uitstel tot eind 2022. Vandaar dat deze auditronde nog steeds gaande is. Over drie jaar mag iedereen zich opmaken voor de volgende ronde externe audits. Ondertussen is het ook nog steeds de bedoeling dat u jaarlijks interne audits laat uitvoeren.

Externe audits moeten passend zijn

Als FG van meerdere gemeenten ben ik de eerste die het nut van audits onderschrijft, maar dan moeten ze wel passend zijn en dienstbaar zijn aan de doelstellingen van het gegevens-beschermingsrecht volgens EU-verordening 2016/679 (AVG) en EU-richtlijn 2016/680 (Richtlijn 680). Richtlijn 680 is een verbijzondering van de AVG voor situaties waarin verwerking van persoonsgegevens plaatsvindt in relatie tot strafbare feiten.

Het leeuwendeel van gemeentelijke taakuitoefening valt onder het regime van de AVG. Maar in enkele gevallen verwerken ook gemeenten informatie over strafbare feiten, dus onder Richtlijn 680. Denk bij dit laatste met name aan bekeuringen door geüniformeerde BOA's, dossiervorming voor het OM door de leerplichtambtenaar, de sociale recherche of opsporing van milieucriminaliteit door de omgevingsdienst.

In tegenstelling tot de AVG, die als EU-verordening rechtstreeks kracht van wet heeft, moest Nederland er iets op verzinnen om Richtlijn 680 te effectueren via nationale wetgeving. Alleen is daar in de periode 2016-2018, toen Richtlijn 680 moest worden ingevoerd, niet goed over nagedacht (vandaar dat er nu weer herzieningen in gang zijn gezet). Gemakshalve zijn gemeenten toen gelijkgeschakeld met de politie via de Wet politiegegevens.

Gemeenten verschillen naar hun aard fundamenteel van de politie, wat ook geldt voor gemeentelijke informatierisicoprofielen – ook al is Richtlijn 680 van toepassing. Het was slimmer geweest om in de Uitvoeringswet AVG te bepalen dat instanties in de bestuurlijke sfeer, die bevoegd zijn om informatie over strafbare feiten te verwerken, ook gehouden zijn aan naleving van Richtlijn 680.

In essentie zijn de AVG en Richtlijn 680 dezelfde regelingen, waardoor je in de uitvoering nauwelijks het verschil merkt. Richtlijn 680 wordt er door de AVG vooral begrijpelijker op. Het gemeentelijk beschermingsbeleid, het privacybeleidskader, leent zich prima voor beide toepassingsgebieden en voorkomt ook dubbeling, zoals FG-aanwijzing onder de AVG én FG-aanwijzing volgens Richtlijn 680.

Met name de afspraken over DPIA's - en bijbehorende risicoprofielen volgens de Schaal van Erg helpen: op basis hiervan verplicht de gemeente zich 'automatisch' tot onder meer het organiseren van audits.

Zie hiervoor de volgende tabel in het gemeentelijk gegevensbeschermingsbeleid (lichte variaties zijn geen probleem zolang de basisgedachte maar wordt aangehouden):

Risicoprofiel	Type audit	Frequentie	Afschrift FG
A1	Quick scan	5 jaarlijks	-
A2	Zelfevaluatie	4 jaarlijks	Vrijwillig
A3	Audit	3 jaarlijks	Ja
B1	Zelfevaluatie	5 jaarlijks	Ja
B2	Zelfevaluatie	4 jaarlijks	Ja
B3	Audit	3 jaarlijks	Ja
C1	Audit	4 jaarlijks	Ja
C2	Audit	3 jaarlijks	Ja
C3	Audit	2 jaarlijks	Ja

Wezenlijk hier, is dat het risicoprofiel aangeeft wanneer een audit passend is. 'Passend' is hét criterium voor behoorlijke naleving van de AVG / Richtlijn 680. In de situaties dat er geen audits nodig zijn, zijn audits niet passend – en daarmee strijdig met de AVG / Richtlijn 680 (disproportioneel).

Audits zijn kostbaar en vergen de nodige tijd en energie. Die investering is alleen gevergd wanneer dat zorgvuldigheidshalve geboden is in het kader van behoorlijk bestuur (goed eigenaarschap). Hoge risicoprofielen spelen met name in het sociaal domein en zijn ook voorspelbaar bij sommige vormen van taakuitoefening op het gebied van openbare orde en veiligheid.

Problematische aspecten RPA

Kortom; voor gemeenten die op deze manier te werk gaan, is de ministeriële regeling periodieke audit politiegegevens overbodig. De RPA werkt zelfs verstorend omdat deze voorziet in één generieke auditverplichting, in het voorbijgaan aan de vraag of en op welke manier dat passend is. Niet alle gegevensverwerkingen in de zin van Richtlijn 680-verwerkingen zijn even risicovol. Daarmee staat de RPA die – niet onbelangrijk – dateert uit 2008, op gespannen voet met de huidige EU-privacywetgeving.

Een ander probleem van de RPA is de status die impliciet aan de audit en de auditor wordt toegekend. Artikel 2 RPA in combinatie met artikel 5 conflicteren qua formulering en opdracht met het FG-toezicht volgens artikel 37-39 AVG / 32-34 Richtlijn 680. *Het zijn de FG's* die in onafhankelijkheid en op basis van hun expertise en kennis van de praktijk 'vanuit de 3e lijn' de naleving van de AVG en Richtlijn 680 controleren, met inbegrip van toezicht op de in artikel 2 RPA bedoelde EDP/IT-audits.

Daarmee is de huidige WPG-auditaanpak niet alleen een doublure,[1] maar heeft Nederland via RPA iets geregeld dat Europeesrechtelijk niet kán. Dat zie je ook aan de eerste prille voorstellen van de Europese Commissie voor de AVG / Richtlijn 680 destijds, die oorspronkelijk ook een bepaling over auditing bevatten. Tijdens het wetgevingsproces werd dit geschrapt, terwijl de bepalingen over de FG het wél haalden. Om het typisch privacyjuridisch te formuleren: naar EU-maatstaven is er voor de huidige WPG-audits geen wettelijke grondslag.

[1] 'Audit' betekent het controleren van een organisatie (onafhankelijke beoordeling door een expert). De FG is bij wet de toezichthouder / beoordelaar voor AVG- / Richtlijn 680-naleving. Vgl. de accountant als auditor op financieel gebied.

Deze RASCI-tabel helpt om de wettelijke rollen en verantwoordelijkheden scherper te onderscheiden.

RASCI	3/4-lines	Eigenaarschap
R – Operationeel verantwoordelijk	1	Directie / MT ('proceseigenaren', ook bij uitbesteding van taken aan aanbieders van informatiediensten en gemeenschappelijke regelingen)
A – Bestuurlijk verantwoordelijk	1	College, Raad, Burgemeester (de bestuursorganen)
S – Ondersteunend	2	Informatiebeheer, risicomanagement, inkoop, communicatie, juridische zaken, concerncontrol, privacyofficer
C – Toezicht	3	FG (evt. geassisteerd door auditors)
I – Geïnformeerd	4	Raad (t.b.v. horizontaal toezicht) Inwoners Landelijk toezicht, met name de Autoriteit Persoonsgegevens

Wat de RPA niet in de laatste plaats problematisch maakt is het bijeffect dat de beroepsorganisatie NOREA die in de RPA wordt gepromoot, buiten de waarborgen van het FG-expertiseprofiel om (artikel 37.5 AVG / 32.2 Richtlijn 680), een eigen en nogal uitvoerig auditraamwerk heeft ontwikkeld waar gemeenten nu mee te maken hebben. Dat is meten met de verkeerde maat.

Gerichte audit

De EDP/IT-audits waarover in de RPA wordt gesproken vallen enkel op hun plek wanneer ze begrepen worden als de toetsing volgens artikel 35.11 AVG. In de terminologie van het gemeentelijk beschermingsbeleid zijn dit de audits die de proceseigenaar moet laten uitvoeren wanneer uit de DPIA blijkt dat audits passend zijn vanwege het risicoprofiel (zie eerdere tabel).

Dat betekent dat er gerichtere auditopdrachten moeten worden verstrekt en audits sterk kunnen worden vereenvoudigd. Want het enige wat nodig is, is antwoord op de volgende drie vragen:

A. **Bestaan** – In welke mate zijn de beheersmaatregelen uit de DPIA geïmplementeerd en gedocumenteerd in een 'procesplan', en is aan de hand hiervan ook het verwerkingregister (zie artikel 30 AVG / 24 Richtlijn 680) geactualiseerd?
B. **Opzet** – In welke mate blijkt uit de DPIA dat deze is doorlopen in de vier fasen volgens artikel 35.7 AVG, met vooral aandacht voor fase 3 (objectieve risicobeoordeling) en fase 4 (lijst van passende maatregelen om de risico's te mitigeren), inclusief risicoclassificatie volgens de Schaal van Erg?
C. **Werking** – In welke mate rapporteert de proceseigenaar binnen een managementcyclus (zoals de planning- en controlcyclus) aan het eindverantwoordelijke bestuursorgaan (de verwerkingsverantwoordelijke), over de uitvoering van de DPIA, implementatie van beheersmaatregelen, actualisering van het verwerkingsregister, evaluatie en bijsturing?

Voor zowel de gemeente als de FG is dat nuttige input. Zolang afspraken worden nagekomen, is er geen reden om de AP te betrekken. Pas als de FG structurele tekortkomingen vaststelt waardoor personen ernstige risico's lopen of in de uitoefening van hun rechten worden belemmerd, is het aan

hem om eventueel de AP om hulp te vragen, overeenkomstig artikel 39.1d AVG / 34d Richtlijn 680 en de principes van systeemtoezicht.

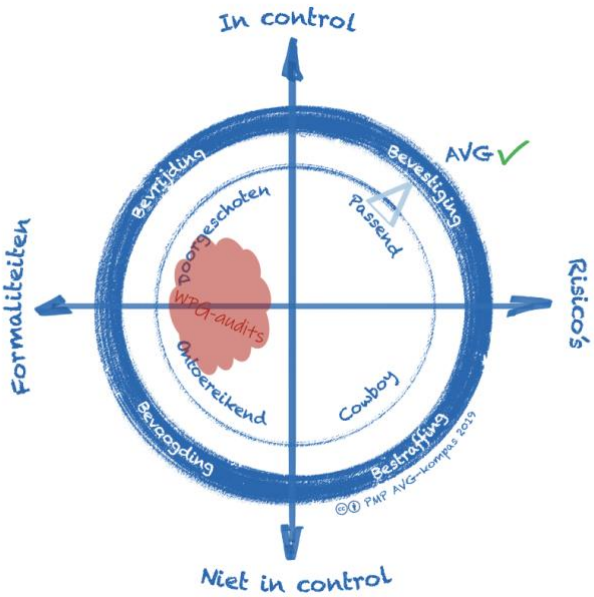
Vóór dat moment is het contraproductief om afschriften van auditrapporten naar de AP te sturen. De bedoeling van auditrapporten is dat ze in staat stellen om verbetermaatregelen te nemen. Bij *good governance* gebeurt dat (lerende organisatie), en verdient de gemeente daarvoor de ruimte en het vertrouwen.

Het hiernavolgende auditplan in de bijlage is nadere concretisering van het voorgaande.

Beoordeling huidige WPG-auditaanpak

Wil er sprake zijn van juiste naleving van de AVG en Richtlijn 680, behoren maatregelen passend te zijn gelet op de risico's, aard, omvang, context en verwerkingsdoeleinden. Of en op welke manier externe audits wél passend zijn, is afhankelijk van de uitkomsten van goede DPIA's. Een wél passende audit bevindt zich in het rechtsboven-kwadrant van onderstaand kompas.

Om de redenen die ik gaf in deze notitie, is de huidige WPG-auditaanpak echter **niet passend** en zelfs in strijd met de wet (EU-wetgeving). De tijd, geld en energie die in de audits wordt gestoken betreft ondoelmatige en ondoeltreffende besteding van middelen.



Bijlage: Auditplan

Aanvulling op het gemeentelijk privacybeleidskader

1) Proceseigenaren van werkprocessen waarin informatie over strafbare feiten wordt verwerkt (bijvoorbeeld 'APV-boeteverlening'), vullen voor ieder werkproces dit quick scan-formulier in. Doe dit in Word. De velden en keuzemenu's laten zich dan gemakkelijk invullen. Dat kan in enkele minuten.
2) Proceseigenaren delen ingevulde formulieren met de privacyofficers. De privacyofficers verifiëren het risicoprofiel zoals deze blijkt uit de beantwoording van vragen 4 en 5 van het quick scan-formulier.
3) Als het goed is, is op de betreffende werkprocessen een DPIA uitgevoerd. Als dat inderdaad het geval is, vergelijken de privacyofficers de risicoscoring uit de quick-scan met de risicoscoring uit de DPIA. Bij afwijkingen kan het zijn dat de DPIA niet actueel genoeg meer is. Draag in ieder geval zorg voor vermelding van de meest realistische 'bruto' risicoscore (het risico bij volledige afwezigheid van beheersmaatregelen).
4) Proceseigenaren en privacyofficers verifiëren gezamenlijk de actualiteit, juistheid en volledigheid van het verwerkingregister aan de hand van de vereisten volgens artikel 30 AVG / 24 Richtlijn 680 en de vermelding van de risicoscore.
5) De privacyofficers stellen een lijst op van matches, afwijkingen en hiaten tussen de uitkomsten van de quick scans en DPIA's, en vermelden bij afwijkingen of hiaten hun voorstellen voor vervolgacties.
    a) De gecomplementeerde lijst bespreken zij met de FG. Voor dit gesprek wordt ook concerncontrol uitgenodigd.
    b) Met name van belang is dat in dit gesprek aan de hand van de risicoscoring duidelijk wordt op welke proceseigenaren een auditverantwoordelijkheid rust volgens het gemeentelijk privacybeleid (zie de daarin opgenomen audittabel).
    c) De uitkomsten van dit gesprek worden gedeeld met de algemeen directeur van de gemeente.
6) De algemeen directeur ziet erop toe dat proceseigenaren bij concerncontrol een auditaanvraag indienen voor toetsing van bescherming van persoonsgegevens bij informatieverwerking die volgens de risicoscoring hiervoor in aanmerking komt.
    a) De aanvraag betreft bestaan, opzet en werking van beheersmaatregelen volgens de gerichte auditopdracht zoals beschreven in de Toelichting van deze notitie.
    b) De audit wordt uitgevoerd door een onafhankelijke, professionele auditor. Concerncontrol kan de audit organiseren via een extern bureau.
    c) De auditor doet verslag van zijn bevindingen aan de proceseigenaar en concerncontrol, met afschrift van het auditrapport aan de FG.
7) Bij vaststelling van gebreken stelt de proceseigenaar met urgentie (immers hoge risicoclassificatie) en in afstemming met concerncontrol en de privacyofficers, een SMART-geformuleerd verbeterplan op.
    a) Aan het verbeterplan wordt na vaststelling per direct uitvoering gegeven.
    b) Zo snel mogelijk maar uiterlijk binnen 6 maanden zijn de verbetermaatregelen doorgevoerd.
    c) De proceseigenaar rapporteert binnen die periode aan de algemeen directeur over de stand van zaken (in control-verklaring), met afschrift aan de FG.
8) De FG gebruikt de quick scan-lijst, auditrapporten en in control-verklaringen als input voor zijn jaarlijkse beoordeling van het gemeentelijk beschermingsbeleid en zijn verslag hierover aan het gemeentebestuur.
9) De privacyofficers dragen zorgen voor de planning en het organiseren van de gesprekken.
10) Dit auditplan is onderdeel van de gemeentelijke planning- en controlcyclus. Het auditplan is van overeenkomstige toepassing op werkprocessen die niet onder Richtlijn 680 vallen, maar waarbij evengoed gegevensverwerking plaatsvindt met een hoog risicoprofiel. Doorloop hiervoor vanaf 2023 dezelfde stappen.

De FG heeft tot taak om te adviseren over en toe te zien op de naleving van Verordening 2016/679 (AVG), EU-richtlijn 2016/680, gerelateerde wet- en regelgeving en het gegevensbeschermingsbeleid van de gemeente. Dit doet hij in onafhankelijkheid en in samenwerking met de Autoriteit Persoonsgegevens. Hij let in het bijzonder op de risico's voor de rechten en vrijheden van personen. Tot zijn verantwoordelijkheden hoort ook toezicht op audits (zie artikel 39.1b AVG / 34b Richtlijn 680).

FG's zijn aangewezen op grond van hun professionele kwaliteiten, in het bijzonder hun expertise op het gebied van het gegevensbeschermingsrecht en de praktijk. Dit FG-advies vloeit dan ook voort uit toepassing van het EU-publiekrecht - met name het EU Handvest Grondrechten, de AVG en Richtlijn 680 en de richtsnoeren van het EU-comité voor interpretatiecoördinatie, de EDPB. Voor herziening is ruimte bij valide argumenten binnen hetzelfde stramien.

Met Nederlandse wet- en regelgeving is rekening gehouden, met voorrang aan het Unierecht bij onduidelijkheid, dubbelzinnigheid of tegenstrijdigheid. Ook opvattingen en advies van anderen zijn meegenomen, voor zover dat past binnen de bedoeling, het systeem en de bewoording van de AVG / Richtlijn 680.

Dit advies is een FG-aanwijzing in de zin van overweging 77 AVG.

#LeesdeAVGbeter

Privacy
Management
Partners
Coöperatie UA
adres
Vondellaan 58
3521 GH Utrecht
telefoon
+31 85 401 38 66
e-mail
info@pmpartners.nl
website
www.pmpartners.nl