

Raadsinformatiebrief

Van	Burgemeester en Wethouder	Zaak nr.	643712
Aan	Gemeenteraad	RIB nr.	2020-27
Portefeuillehouder	K.J. Walters	Datum	28 mei 2020
Informatie bij	J. van Straalen	Tel. nr.	(035) 629 2068

Onderwerp

Jaarverslag Functionaris Gegevensbescherming (FG-Verslag 2019)

Kernboodschap

Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Een belangrijke eis van de AVG is onder andere dat overheidsorganisaties een Functionaris Gegevensbescherming (FG) aanstellen, zo ook de gemeente Hilversum.

De FG is de onafhankelijke wettelijke toezichthouder, op basis van artikel 35-37 AVG. Artikel 38, lid 3 AVG, verplicht de FG te rapporteren over zijn bevinden in hoeverre de Gemeente Hilversum voldoet aan de eisen van de AVG. Deze bevindingen zijn terug te lezen in de bijlage “FG-Verslag 2019.”

2019 is het tweede jaar waarover de FG een verslag uitbrengt en in het kort zijn beoordeling:

“Gemeente Hilversum boekte in 2019 minder voortgang in de uitvoering van het AVG- werkprogramma dan gepland. Door personele uitval binnen het Privacy & Informatieveiligheid Team (PIT), ontbrak het de gemeente aan slagkracht en werden structureel gestelde doelen niet gehaald.

Het gemankeerde PIT bleef evenwel goed functioneren op het niveau van vraag-gestuurde ondersteuning aan de gemeenteorganisatie en afhandeling van verzoeken of klachten. Inwoners en medewerkers bleven onverminderd toegang behouden tot AVG-dienstverlening, zoals de mogelijkheid om inzage- en correctierechten uit te oefenen en contact met de functionaris gegevensbescherming. Ook hebben zich geen ernstige incidenten voorgedaan.

Wat vertrouwen schept is dat de gemeente – met name ook vanwege haar aandacht voor procesgericht werken en concern control – veel in huis heeft om de opgelopen vertraging weer weg te kunnen werken. De manier waarop het smart city-beleid met privacy waarborgen wordt omkleed is een compliment waard. Niet in de laatste plaats dient vermeld te worden dat het PIT is versterkt met professionals op het gebied van privacy en informatiebeveiliging.

Vanuit toezichtsperspectief verdient Gemeente Hilversum daarom onderkenning van de tegenslag in 2019 (personele uitval is altijd belemmerend) en het vertrouwen dat doelen in 2020 wél worden gehaald.

Naar verwachting heeft de gemeente nog enkele jaren nodig om over de volle breedte op het kwaliteitsniveau van de AVG te komen. De snelheid waarmee dat gaat, is niet alleen afhankelijk van het PIT maar is met name ook afhankelijk van bestuurlijke support en interne verantwoordingsafspraken. In 2019 werden op deze punten hernieuwde afspraken gemaakt in het overkoepelende Privacy Beleid 2020-2024.”

Aanleiding

De FG is de onafhankelijke wettelijke toezichthouder op basis van artikel 35-37 AVG. De FG brengt rechtstreeks verslag uit aan het College van B&W. In dit jaarverslag over 2019 rapporteert hij over zijn bevindingen in hoeverre de gemeente Hilversum voldoet aan de eisen van de AVG. Door middel van dit jaarverslag wordt verzekerd dat het College van B&W op de hoogte is van zijn advies en aanbevelingen. Dit is onder andere uitgewerkt in de paragraaf “Ontwikkellijn algemene beleidsvoering”.

Dit verslag is dan ook bedoeld om u te informeren over de bevindingen van de FG.

Vervolgtraject

De aanbevelingen van de FG over 2019 zijn door het College overgenomen. Dat houdt het volgende in:

- Het werkprogramma AVG wordt vervolgd en aan de meerjarenplannen wordt uitvoering gegeven.
- Er is een prioritering aan de Data Protection Impact Assessment (DPIA) gegeven op de meest risicovolle processen (sociaal domein en openbare orde en veiligheid).
- Procedures en werkinstructies worden opgesteld, of herijkt en herzien.
- Mandaatregelingen in buiten-gemeentelijke gegevensverstrekkingen worden onderzocht op actualiteit.
- Privacy en informatieveiligheidsvraagstukken worden besproken in het Privacy en Informatieveiligheid Team (PIT) en waar nodig met de externe FG.
- Directie en de wethouder worden periodiek op de hoogte gesteld over de ontwikkelingen.
- Door middel van de “Raadsweekbrieven Corona” wordt de raad geïnformeerd over de waarborgen omtrent privacy en informatieveiligheid in de Corona-tijd.

Burgemeester en wethouders van Hilversum,
de gemeentesecretaris,

de burgemeester,

D. Emmer

P.I. Broertjes

Bijlage(n): FG-verslag 2019

Deze raadsinformatiebrief is digitaal beschikbaar op [internet](#) onder “Vergaderstukken”, B&W-vergadering 26 mei 2020

FG-verslag 2019-2020



Aan: het college van B&W Gemeente Hilversum

Van: de functionaris gegevensbescherming

Beoordeling

Gemeente Hilversum boekte in 2019 minder voortgang in de uitvoering van het AVG-werkprogramma dan gepland. Door personele uitval binnen het Privacy & Informatieveiligheid Team (PIT), ontbrak het de gemeente aan slagkracht en werden structureel gestelde doelen niet gehaald.

Het gemankeeerde PIT bleef evenwel goed functioneren op het niveau van vraaggestuurde ondersteuning aan de gemeenteorganisatie en afhandeling van verzoeken of klachten. Inwoners en medewerkers bleven onverminderd toegang behouden tot AVG-dienstverlening zoals de mogelijkheid om inzage- en correctierechten uit te oefenen en contact met de functionaris gegevensbescherming. Ook hebben zich geen ernstige incidenten voorgedaan.

Wat vertrouwen schept is dat de gemeente – met name ook vanwege haar aandacht voor procesgericht werken en concerncontrol – veel in huis heeft om de opgelopen vertraging weer weg te kunnen werken. De manier waarop het smart city-beleid met privacywaarborgen wordt omkleed is een compliment waard. Niet in de laatste plaats dient vermeld te worden dat het PIT is versterkt met professionals op het gebied van privacy en informatiebeveiliging.

Vanuit toezichtsperspectief verdient Gemeente Hilversum daarom onderkenning van de tegenslag in 2019 (personele uitval is altijd belemmerend) en het vertrouwen dat doelen in 2020 wél worden gehaald.

Naar verwachting heeft de gemeente nog enkele jaren nodig om over de volle breedte op het kwaliteitsniveau van de AVG te komen. De snelheid waarmee dat gaat, is niet alleen afhankelijk van het PIT maar is met name ook afhankelijk van bestuurlijke support en interne verantwoordingsafspraken. In 2019 werden op deze punten hernieuwde afspraken gemaakt in het overkoepelende Privacy Beleid 2020-2024.

Utrecht, 3 april 2020

A handwritten signature in black ink, appearing to be 'S.H. Katus', written over a horizontal line.

mr. S.H. Katus, CIPP/E CIPM FIP
Functionaris gegevensbescherming

Privacy Management Partners

Vondellaan 58, 3521 GH Utrecht

E: info@pmpartners.nl

T: 085 401 38 66

W: www.pmpartners.nl

Leeswijzer

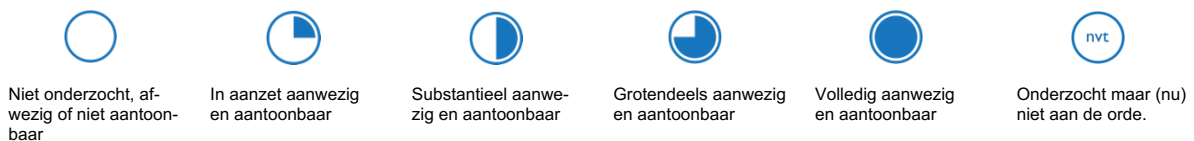
De Algemene Verordening Gegevensbescherming (AVG) gaat over de doelmatigheid en doeltreffendheid van praktische waarborgen rondom de gemeentelijke bedrijfsprocessen die afhankelijk zijn van persoonsgegevens. Gemeente Hilversum respecteert het recht op bescherming van persoonsgegevens wanneer de praktische waarborgen weloverwogen zijn genomen, en personen hierdoor passend worden beschermd tegen de keerzijden van de gegevensverwerking.

Prestatieindicatoren

De gemeente wordt getoetst op de naleving van de AVG op basis van de tien kritische prestatieindicatoren (KPI's) die logischerwijs uit de AVG voortvloeien. Zie de bijlagen voor nadere toelichting.

De toetsing verloopt volgens de jaarcyclus van de functionaris gegevensbescherming, waarbij de FG zowel structureel als incidenteel de vinger aan de pols houdt van de AVG-beleidsvoering. Structurele toetsing vindt plaats via het reguliere contact met het PIT en de jaarlijkse AVG-audit. Incidentele toetsing bestaat uit FG-advisering bij DPIA's en FG-betrokkenheid bij klachten en incidenten.

Dit FG-verslag geeft het beeld weer van de gemeentelijke AVG-beleidsvoering zoals die in de loop van het jaar is gebleken. Aan de hand van drie taartgrafiekjes wordt per KPI de doelmatigheid en doeltreffendheid van de aanpak gevisualiseerd, door de scoring te duiden ten aanzien van 'opzet' (de maatregelen kloppen op papier), 'bestaan' (de maatregelen worden daadwerkelijk in praktijk gebracht) en 'werking' (de maatregelen blijken in de praktijk ook afdoende/voldoende passend).



Ontwikkellijn

De tien KPI's vormen samen een gelaagde ontwikkellijn. De eerste laag is de bestuurlijke ontwikkellijn die laat zien hoever de gemeente gevorderd is in de nakoming van artikel 24 AVG (ontwikkellijn algemene beleidsvoering). De tweede laag is de ontwikkellijn op het niveau van de gemeentelijke werkprocessen, waarbij de vraag centraal staat in hoeverre de gemeente voldoet aan artikel 25 AVG. Deze tweede ontwikkellijn vormt tevens de koppeling met het register dat de gemeente conform artikel 30 AVG bijhoudt.¹

De verbinding tussen beide ontwikkellijnen wordt vooral gevormd door punt 5 'privacy by design', punt 6 'ketenregie' en punt 7 'veerkracht' op de bestuurlijke ontwikkellijn. Op deze drie punten wordt resultaat geboekt wanneer de ontwikkellijn per aandachtgebied daar voldoende aanleiding toe geeft.

Relatie met de planning en control-cyclus

Het FG-verslag ondersteunt de verantwoording door het college van B&W aan de raad en eventueel anderen. Daarnaast beschikt de accountant op deze manier over een in onafhankelijkheid afgegeven beoordeling van de gemeentelijke AVG-beleidsvoering.

¹ In lijn met afspraken die zijn gemaakt in VNG-verband. Zie: <https://www.informatiebeveiligingsdienst.nl/nieuws/vooringevuld-verwerkingsregister-gemeenten/>

Begrippen

<i>AVG</i>	Algemene Verordening Gegevensbescherming
<i>Bestuurlijk privacybeleid</i>	Beleidskader, werkprogramma en ter beschikking stelling van middelen
<i>BIO</i>	Baseline Informatiebeveiliging Overheid
<i>CISO</i>	Chief information security officer, degene die de gemeentelijke informatiebeveiliging coördineert
<i>FG</i>	Functionaris voor gegevensbescherming, wettelijk toezichthouder volgens artikel 37-39 AVG
<i>DPIA</i>	Data protection impact assessment, de AVG-risicoanalyse die aan een procesplan vooraf gaat
<i>PIT</i>	Privacy en informatieveiligheid team (PIT) - het ondersteuningsteam van de gemeente
<i>PO</i>	Privacy officer (degene die de uitvoering van het AVG-beleid coördineert)
<i>Portefeuillehouder</i>	Collegelid dat namens het college de AVG-beleidsvoering bewaakt
<i>Procesplan</i>	de documentatie van concrete organisatorische en technische oplossingen voor de bescherming van persoonsgegevens op operationeel niveau (vervolg op een DPIA)
<i>Privacy by design</i>	De implementatie/realisatie van organisatorische en technische beheersmaatregelen voor de bescherming van persoonsgegevens (vervolg op een procesplan)
<i>Risicoprofiel</i>	Waardering van AVG-risico's, voor de duidelijkheid uitgedrukt in DPIA-scores variërend tussen 0 en C3 volgens de AVG-risicomatrix die de gemeente hanteert.
<i>Werkprogramma</i>	Het meerjarenplan van de gemeente voor AVG-transitie, opgedeeld in jaarplannen.

Ontwikkellijn algemene beleidsvoering

Speerpunten	Opzet	Bestaan	Werking	Advies
1. Beleid				Het college is akkoord met privacybeleid waarin bescherming van persoonsgegevens via eigenaarschap, risicosturing, transparantie en rekenschap nu beter aansluit bij de AVG. De smart city-aanpak waarbij de dialoog met inwoners wordt opgezocht, laat zien dat 'privacy' vooral een manier is om gedragen oplossingen te vinden. De effectuering van het privacybeleid is in gang gezet. Pak hierop door.
2. Regie en support				Door uitval van de privacy officer ontstond een situatie waarin het PIT de slagkracht miste om uitvoering te geven aan het werkprogramma, afgezien van de beleidsupdate. De gemeente ging evenwel op zoek naar oplossingen en heeft die ook gevonden. Bovendien lijkt synergie te ontstaan met de al bestaande aanpak procesgericht werken. De vernieuwde teamsamenstelling van het PIT schept vertrouwen. Het PIT moet nu vooral aan de slag met de DPIA's
3. Toezicht				De gemeente beschikt over een gekwalificeerde FG. Deze werd in 2019 betrokken bij vragen en incidenten, meedenken over oplossingen voor het PIT en bij de smart city-aanpak. In december 2019 informeerde hij het college via een tussenrapportage over de vertraging in het AVG-werkprogramma vanwege de tegenslag bij het PIT. Betrek de FG nog meer bij de gemeentelijk datastrategie.
4. Werkprogramma				Vanwege de tegenslag van het PIT, is de uitvoering van het werkprogramma achter gebleven, uitgezonderd de beleidsupdate. Het jaarplan 2019 verschuift daarom naar 2020. Het zwaartepunt ligt nu bij DPIA's. Door synergie met procesgericht werken en informatiebeveiliging, is wellicht versnelling mogelijk.
5. Privacy by design				AVG-optimalisatie van gemeentelijke werkprocessen m.b.v. DPIA's start vanwege de hiervoor genoemde vertraging pas in 2020. Prioriteer processen met het hoogste AVG-risicoprofiel (sociaal domein, veiligheid, ondermijning, fraudebestrijding, enzovoorts).
6. Ketenregie				Scoring op dit punt verdient de gemeente met de smart city-aanpak en herijking van de samenwerking met Parkeerservice en woningcorporaties. AVG-optimalisatie van overige vormen van ketensamenwerking moet nog plaatsvinden. Gebruik DPIA's ook om op dit vlak in passende maatregelen te voorzien.
7. Verzoeken, klachten en incidenten (veerkracht)				De gemeente heeft in 2019 adequaat ingespeeld op verzoeken, klachten en incidenten. Waar nodig werd de FG goed betrokken. Voer een incidentmanagement-aanpak die de totale AVG-beleidsvoering dekt. De datalekken-administratie is een startpunt. Leer van incidenten en stel bij waar dat kan.
8. Communicatie en training/opleiding				Ontwikkel met de afdeling communicatie een structurele aanpak voor het op peil brengen en houden van kennis en gedrag (cultuur). Waarborg dat informatieverstrekking aan personen bij verkrijging van persoonsgegevens door de gemeente steeds voldoet aan de eisen van artikel 12-14 AVG.
9. Informatiebeveiliging				Gemeente Hilversum werkt aan de overgang naar de BIO.
10. Budget				In 2019 was er voldoende budget.

Ontwikklijn gegevensbescherming werkprocessen²

Aandachtsgebied	Opzet	Bestaan	Werking	Advies
1. Belastingheffing				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
2. Bescherming en opvang				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
3. Burgerzaken				Er worden al langere tijd strenge eisen gesteld aan BRP en BSN, maar nog niet zozeer vanuit de AVG. Hanteer daarom evengoed een DPIA-aanpak om een beeld te vormen van de passendheid van maatregelen.
4. Cultuur en sport				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
5. Fraudeonderzoek				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
6. Gemeenteraad				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
7. Interne organisatie				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
8. Jeugd en onderwijs				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
9. Lokale economie				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
10. Milieu en duurzaamheid				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
11. Ruimte en bereikbaarheid				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
12. Veiligheid en openbare orde				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
13. Werk en inkomen				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.
14. Zorg en welzijn				Voer DPIA's uit voor zover sprake is van verwerking van persoonsgegevens met een hoger risicoprofiel (> A1). Realiseer en implementeer procesplan(nen) waar nodig.

² Indeling naar VNG-aanbeveling – zie vorige voetnoot. Clustering op hoofdthema's biedt totaaloverzicht en helpt verkokering tegen te gaan.

Toelichting

De kwetsbaarheid van privacybeleidsvoering komt aan het licht wanneer de mensen uitvallen die het beleid handen en voeten helpen geven. De privacy officer van de gemeente Hilversum was in het afgelopen jaar langdurig uitgeschakeld. Geschikte vervanging was op dat ogenblik niet voorhanden. De overige leden van het PIT bewaakten weliswaar goed het fort maar het werkprogramma voor de AVG-transitie kwam stil te liggen. Als gevolg hiervan zijn er geen DPIA's uitgevoerd voor het op AVG-niveau brengen van de werkprocessen, zoals voorgenomen en valt er geen voortgang te rapporteren op de ontwikkellijn voor de werkprocessen.

Hiermee is niet gezegd dat de bescherming van persoonsgegevens in het slop is geraakt. De gemeente heeft op twee punten wezenlijke resultaten geboekt.

1. In de eerste plaats is dat de herijking van overkoepelend privacybeleid voor de hele gemeente, wat heeft geleid tot doelmatigere en doeltreffendere beleidsafspraken in het Privacy Beleid 2020-2024, waar het college mee akkoord is gegaan.
2. In de tweede plaats heeft het college, in samenspraak met de raad, via de smart city-beleidsvoering op laten zien hoe privacy en openbaar bestuur met elkaar in balans kunnen worden gebracht. De smart city-aanpak wordt gekenmerkt door transparantie en dialoog, waarbij bescherming van persoonsgegevens is gaan behoren tot de leidende principes. Het besluit tot inrichting van een inwonerpanel om mee te denken over privacyvriendelijke oplossingen, was verstandig. De aanpak tot nu toe is in de geest van de AVG. Daarmee heeft de gemeente heeft in 2019 voortgang geboekt op het vlak van leren inspelen op de AVG.

Ook het AVG-serviceniveau bleef op peil; het PIT bleef verzoeken, klachten en incidenten afhandelen zoals gebruikelijk. Inwoners en medewerkers konden ook onverminderd blijven rekenen op tussenkomst door de FG bij serieuze problemen op het gebied van gegevensbescherming. Van die regeling hoefde gelukkig geen gebruik te worden gemaakt.

Inmiddels heeft de gemeente het PIT weer weten te versterken door [tijdelijk te voorzien in extra capaciteit](#). [Nog onderzocht moet worden onderzocht wat voor de juiste ondersteuning van de gemeente de gewenste sterkte van het PIT moet zijn](#). Belangrijk is daarnaast ook dat de verbinding is gevonden tussen AVG-beleidsvoering en initiatieven voor verdere optimalisatie van de gemeentelijke bedrijfsvoering ('Procesgericht werken'). Want er zijn veel raakvlakken.

Dit alles overziend, beschikt de gemeente over de middelen om de achterstand weg te werken die vorig jaar werd opgelopen. Maak hierover duidelijke afspraken door het stellen van doelen en deadlines. Met de uitvoering van DPIA's worden meerdere vliegen in één klap geslagen: werkprocessen en informatiebehoeften in kaart, ICT-afhankelijkheden worden beter zichtbaar, de risico's voor mens en gemeente worden duidelijk en – meest belangrijk – het wordt voor iedereen helder wat er precies nodig is voor het bieden van passende bescherming van persoonsgegevens, zoals de AVG voorschrijft. Deze aanpak helpt meteen ook om in te spelen op de baseline informatiebeveiliging overheid (BIO).

Beperk het werkprogramma niet alleen tot binnengemeentelijke gegevensverwerking, maar begrijp ook dat de verantwoordelijkheden zich uitstrekken tot buitengemeentelijke gegevensverwerking. Dat wil zeggen; alle gegevensverwerking waarvoor Gemeente Hilversum volgens de AVG eindverantwoordelijk voor is en de aansprakelijkheidsrisico's voor draagt. Denk met name aan gemeenschappelijke regelingen zoals de gemeenschappelijke regeling Regio Gooi en Vechtstreek. Mogelijk blijken eventuele mandaatregelingen niet meer te kloppen.

De AVG en privacybescherming is niet alleen een vraagstuk voor specialisten maar is vooral een bestuurlijke uitdaging. Boven het niveau van tactische en operationele oplossingen, is ook bestuurlijk-strategische visie vereist: wat voor een gemeente wil Hilversum zijn in het digitale tijdperk? Welke keuzes worden er gemaakt over de inzet van nieuwe technologieën zoals data-analyse, kunstmatige intelligentie, profilering, drones en gezichtsherkenning? Hoe verhoudt zich dat tot vraagstukken op het gebied van zorg en welzijn, werk en inkomen, openbare orde en veiligheid, ondermijning, achterstandsproblematiek, fraudebestrijding, volksgezondheid of woningnood – ook rekening houdend met steeds mondiger wordende burgers en (inter)nationale ontwikkelingen?

Het werkt bevorderlijk voor de AVG-beleidsvoering wanneer op bestuurlijk niveau een gemeentelijke strategiegroep wordt ingericht voor het formuleren van antwoorden. Voor zover dit al gebeurt, is het belangrijk om de verbinding te leggen met de AVG-beleidsvoering. Want de AVG is in de kern niets anders is dan dé wet op de data-ethiek. Via DPIA's en dialoog zoals het smart city-inwonerpanel wordt gewerkt aan gedragen oplossingen.

Bijlage I - Nadere informatie over AVG-beleidsvoering

Bescherming van persoonsgegevens is als grondrecht geregeld in artikel 10 Grondwet en artikel 8 EU Handvest van de Grondrechten. Vervolgens is dit bij wet nader uitgewerkt. Meest belangrijk in dit verband is de Algemene Verordening Gegevensbescherming (AVG) van de Europese Unie.

In de AVG staan de verplichtingen van de ‘verwerkingsverantwoordelijke’ centraal (hierna: ‘AVG-verantwoordelijke’). Deze is degene die het grondrecht op gegevensbescherming moet waarborgen. Zonder de inspanningen van de AVG-verantwoordelijke geen bescherming van persoonsgegevens.

In de publieke sector wordt sinds 1998 ervan uitgegaan de AVG-verantwoordelijke het bestuursorgaan is dat voor uitoefening van taken de gegevensverwerking nodig heeft. Het is niet doelmatig en waarschijnlijk verminderd doeltreffend wanneer ieder bestuursorgaan binnen de gemeente eigen privacybeleid voert en ieder afzonderlijk een FG aanwijst. Om praktische redenen wordt daarom gewerkt met één overkoepelend raamwerk voor de bescherming van persoonsgegevens.

Bestuurlijke verantwoordelijkheid

In essentie draait de AVG om goed huisvaderschap ten aanzien van gegevensverwerking waarvoor het college eindverantwoordelijk is (good governance). De hoge boetes in de AVG zijn bedoeld om hieraan te herinneren. Maar tegelijk: wie goed huisvaderschap betracht, heeft niets te vrezen en kan met vertrouwen verantwoording afleggen. Het is de rol van de FG om daarbij te helpen conform artikel 37-39 AVG.

Strategisch belang

De AVG is veel minder een ICT-aangelegenheid of ‘iets voor juristen’ dan de AVG op het eerste gezicht doet vermoeden. De AVG geeft het groene licht aan gegevensverwerkingen. Zonder groen licht is de gegevensverwerking onrechtmatig en moet deze gestaakt worden. Zonder gegevensverwerking geen gemeentebelastingen, burgerzaken, dienstverlening in het sociaal domein, werkgeverschap, fraudeonderzoek, bestuurlijke innovatie met data, enzovoorts. De kunst is om op bestuurlijk niveau AVG-conform te sturen, zodat op uitvoeringsniveau alles in orde komt – én in orde blijft, zodat het licht niet op rood komt te staan.

Kleinigheden doen niet zozeer terzake. Waar de gemeente vooral op moet letten, zo geeft de AVG aan, zijn de gegevensverwerkingen die bij rood licht aanzienlijke of zelfs ernstige risico’s voor personen kunnen betekenen. Zelfs een kleine fout kan voor een individu ernstige gevolgen hebben. Instanties zoals de Nationale Ombudsman en de Algemene Rekenkamer luiden inmiddels de noodklok dat hiervan in de praktijk veel te veel voorbeelden zijn.³ Al in 1998 koppelde de Nederlandse wetgever het aandachtsgebied aan behoorlijk bestuur.

Reikwijdte bestuurlijke verantwoordelijkheid

De verantwoordelijkheden van de gemeente – en daarmee het toezicht van de FG – strekken zich uit tot *alle* gemeentelijke verwerkingen van persoonsgegevens. Dat is niet alleen intern. Ook bij het op afstand laten uitvoeren van taken blijft de gemeente eindverantwoordelijk. Wanneer een gemeente taken uitvoert voor een andere gemeente, is de andere gemeente ‘AVG-verantwoordelijke’. Wanneer gemeenten samenwerken in een gezamenlijke gegevensverwerking zijn zij collectief verantwoordelijk maar zonder nadere afspraken afzonderlijk (‘hoofdelijk’) aansprakelijk.

De AVG is een supranationale wet die alle lagere regelgeving en afspraken *overrulet*.⁴ Daarmee harmoniseert de AVG, waar van toepassing, op dwingende wijze ook de Algemene Wet Bestuursrecht, de Gemeentewet, de Wet Basisregistratie Personen, ministeriele besluiten, provinciale en gemeentelijke verordeningen, contracten, gedragscodes, enzovoorts. Dat vergt

³ Zie [Rapport Basisregistraties](#) van de Algemene Rekenkamer (2014) en het rapport [Zorgen voor Burgers](#) van de Nationale Ombudsman (2019).

⁴ Wel laat de AVG op onderdelen ruimte voor nadere inkleuring via nationale wetgeving, die evenwel nooit met de AVG mogen conflicteren. Een belangrijke wet in dit verband is de NL [Uitvoeringswet AVG](#) (UAVG).

soms ‘omdenken’ bij inkoop/uitbesteding of het onderbrengen van taken bij een gemeenschappelijke regeling. Verantwoordelijkheden kunnen niet worden weggedelegeerd maar blijven onder de AVG de verantwoordelijkheid van het college.

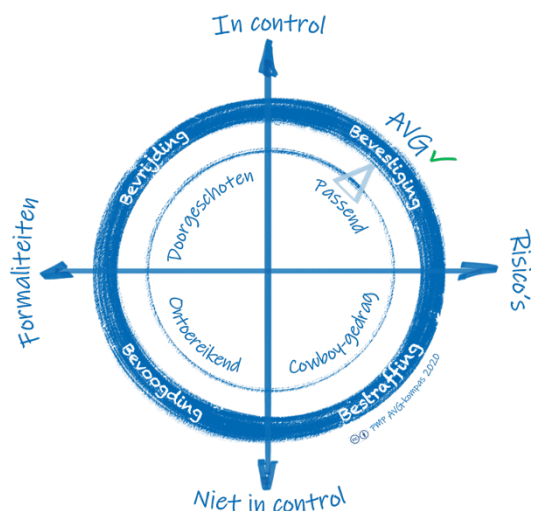
Begrenzing van verantwoordelijkheid

AVG-verantwoordelijkheden houden op na onomkeerbare vernietiging van persoonsgegevens. Bij verzelfstandiging van taken of fusies ontstaan nieuwe AVG-verantwoordelijken met nieuwe verplichtingen. Uit oogpunt van zorgvuldigheid horen de oude AVG-verantwoordelijken zich er dan wel eerst van te verzekeren dat dan ook de nieuwe AVG-verantwoordelijke de bescherming van persoonsgegevens op passende wijze waarborgt. Wanneer gegevens eenmaal zijn verstrekt aan derden zoals zorginstellingen of de Belastingdienst (andere AVG-verantwoordelijken), ontstaat ook daar AVG-verantwoordelijkheid. De gemeente blijft verantwoordelijk voor de eigen gegevens maar is niet meer verantwoordelijk voor dezelfde gegevens die vanaf dat moment onder de hoede van de nieuwe AVG-verantwoordelijke zijn komen te vallen.

Sturen op gegevensbescherming

Om op bestuurlijk niveau zinnig te kunnen sturen op de AVG, is het belangrijk om het voorgaande goed te begrijpen. Meest belangrijk zijn de resultaatsverplichtingen om te voorzien in risicosturing (artikel 24 AVG) zodat op alle fronten sprake is van operationele risicobeheersing (artikel 25 AVG). Al het andere dat wordt voorgeschreven in de AVG, hangt hiermee samen. Dus ook bijvoorbeeld de inrichting van een ‘verwerkingsregister’ en de aanwijzing van een FG, die in artikel 39.2 AVG evenzeer op het hart gedrukt krijgt om op risico’s te letten.

Gegeven die nadruk op risicobeheersing, wordt het een stuk gemakkelijker om door de bomen het bos te zien. Alles wat géén functie heeft in AVG-risicobeheersing is niet AVG-conform. Om aan de AVG te voldoen is daarmee in de eerste plaats belangrijk dat de gemeente de juiste koers aanhoudt (‘rechtsboven’ volgens het hier afgebeelde AVG-kompas). Voor goed begrip kan het woord ‘risico’ overigens het beste worden vervangen door ‘belang’ (bescherming van belangen voor mens en organisatie).



Het AVG-kompas helpt om beleid en operationele oplossingen teijken aan de AVG en om de juiste koers aan te houden. Voldoen aan de AVG is altijd ‘rechtsboven’. De blauwe buitenring verwoordt de stijlen van fair toezicht per kwadrant.

10 hoofdkenmerken

Op basis van het voorgaande en aan de hand van de overige bepalingen in de AVG, kunnen tien hoofdkenmerken worden vastgesteld van AVG-conforme beleidsvoering. Deze vormen de speerpunten van het bestuurlijk dashboard.

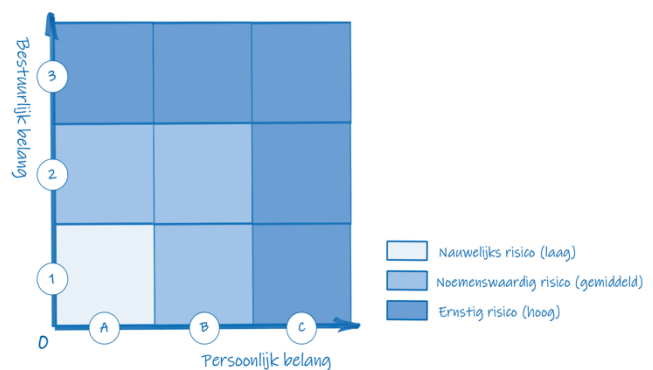
1. **Bestuurlijk beleid** – De AVG-verantwoordelijke opereert aantoonbaar risicogestuurd door middel van formeel vastgesteld privacybeleid met daarin duidelijke verdeling van rollen en verantwoordelijkheden en dat gericht is op voorzien in échte oplossingen voor échte problemen. Het beleid wordt voldoende regelmatig geëvalueerd en geactualiseerd.
2. **Regie & support** – Om tot oplossingen te komen heeft de AVG-verantwoordelijke op bestuursniveau een portefeuillehouder aangewezen. Binnen de organisatie functioneert een multidisciplinair team van professionals (AVG-ondersteuningsteam) voor het realiseren van doelen en ondersteuning van de organisatie onder leiding van een slagvaardige AVG-programmacoördinator.
3. **Toezicht** – De AVG-verantwoordelijke laat zich bijstaan door een gekwalificeerde FG die in onafhankelijkheid zijn werk doet conform de artikelen 37-39 AVG en de organisatie toetst op

- naleving van de AVG, andere relevante wetten en de privacybeleidsvoering volgens deze punten.
4. **Werkprogramma** – De AVG-verantwoordelijke hanteert een werkprogramma op basis van prioriteiten waartoe is besloten op basis van een organisatiebrede AVG-risicoanalyse, en dat flexibel genoeg is om de lessen uit incidenten te verdisconteren.
 5. **Ketenregie** – De AVG-verantwoordelijke waarborgt bescherming van persoonsgegevens op bestuurlijk- of managementniveau bij gegevensverwerking op afstand.
 6. **Privacy by Design** – De AVG-verantwoordelijke draagt ervoor zorg dat aantoonbaar passende maatregelen zijn genomen voor doelmatige en doeltreffende beheersing van risico's per gegevensverwerking/werkproces, op basis van geveenseffectbeoordelingen (PIA's).
 7. **Verzoeken, klachten en incidenten** – De AVG-verantwoordelijke beschikt over procedures voor soepel inspelen op verzoeken, klachten en incidenten, administreert dit en trekt hier lering uit. Verzoeken worden binnen de wettelijke termijn afgehandeld. Voor zover incidenten kwalificeren als datalek, waarborgt de organisatie afhandeling conform artikelen 33 en 34 AVG ('meldplicht datalekken').
 8. **Communicatie & training/opleidingen** – De AVG-verantwoordelijke voert communicatiebeleid voor transparante AVG-beleidsvoering bij alle doelgroepen en het bewerkstelligt een volwassen AVG-organisatiecultuur, mede op basis van bespreekbaarheid, voorbeeldgedrag en aanspreekbaarheid. DPIA's en de vorming van risicodossiers ('procesplannen') worden tevens gezien als 'training en bewustwording'. Waar mogelijk worden oplossingen gezocht in dialoog met de doelgroep. Juist DPIA's kunnen een goed instrument zijn om burgers te betrekken en begrip en draagvlak te creëren.
 9. **Informatiebeveiliging** – De AVG-verantwoordelijke beschikt over sector-conform informatiebeveiligingsbeleid en wordt ondersteund door professionele informatiebeveiligers, die betrokken zijn in het AVG-ondersteuningsteam. Informatiebeveiliging speelt nadrukkelijk een rol bij het realiseren van 'Privacy by Design'.
 10. **Budget** – Voor het realiseren van het bovenstaande zijn steeds voldoende financiële middelen beschikbaar – gebudgetteerd of ad hoc.

AVG-risicomatrix

Volgens de AVG en heersende rechtspraak, vormt verwerking van persoonsgegevens niet meteen een inbreuk op de privacy. Vooral belangrijk is in hoeverre de gemeente heeft voorzien in passende beschermingsmaatregelen.

Wat 'passend' is, is afhankelijk van de vraag hoeveel risico ontstaat als die maatregelen *niet* worden genomen – variërend van voorzienbaar licht ongemak tot desastreuze gevolgen. Hoe voorzienbaarder en heftiger de gevolgen, hoe groter het risico. Bij een A1 volstaan lichte maatregelen. Het andere uiterste, een C3, vergt bijzonder robuuste maatregelen.



De **AVG-risicomatrix** is een hulpmiddel voor het classificeren van privacyrisico's. Zonder AVG-risicoclassificatie is niet duidelijk hoe erg een privacyprobleem nou eigenlijk is. De AVG-risicomatrix staat daarom ook bekend als de *Schaal van erg*.

De functie van DPIA's is om tot de goede balans te komen.⁵

⁵ Goed uitgevoerde DPIA's zijn een objectieve beoordeling in de zin van overweging 76 AVG.

Bijlage II - Nadere informatie over de FG-functie

De FG is door het college aangewezen als toezichthouder op de naleving van de AVG. De positie en taken van de FG zijn bij wet geregeld.⁶ Deze komen erop neer dat de FG in onafhankelijkheid vaststelt op welke punten de gemeente voldoet aan de AVG. Omgekeerd stelt de FG ook vast waar eventueel sprake is van terugval.

In veel opzichten doet de rol van de FG denken aan die van de accountant. Een belangrijk verschil met de accountant is dat een FG advies en toezicht niet mag scheiden maar *moet* combineren. Op deze manier kan hij de gemeente houvast bieden en wordt voorkomen dat hij oplossingen achteraf moet afkeuren. De AVG geeft de FG de missie mee om ‘naar behoren rekening te houdend met de doelen, context en risico’s van gegevensverwerking’. Mocht de kwaliteit te wensen over laten, is het aan de FG om de gemeente te coachen naar betere oplossingen. Bij acute problemen moet de FG deze aankaarten.

Relatie FG/AP

Waar nodig werkt de FG samen met het centrale AVG-toezicht. Voor Nederland is dat de Autoriteit Persoonsgegevens (AP). De FG is voor de AP het contactpunt met de gemeente inzake AVG-aangelegenheden. Zie dit als een complementair toezichtstelsel. Wettelijk is er geen hiërarchische relatie tussen de AP en de FG. Boven beide toezichthouders staat de rechter. Het is de taak van de FG om de AP uiteen te zetten op welke wijze de gemeente Edam-Volendam invulling geeft aan de uitvoering van de AVG (‘bufferfunctie FG’).

Relatie FG/klachtencommissie en gemeentelijke ombudsman

De FG ziet toe op AVG-gegevensbescherming. Personen die in de knel komen door verkeerde gegevensverwerking, hebben wettelijk recht op toegang tot de FG.⁷ De FG vervult in die gevallen een rol die doet denken aan bezwaar en beroep, zij het op basis van de AVG (‘FG-ombudsfunctie’). De klachtencommissie en de algemene gemeentelijk ombudsfunctie beoordelen langs de lijnen van de Algemene wet bestuursrecht de inhoudelijke zorgvuldigheid van gemeentelijk handelen. De FG helpt door de rechtmatigheid, betrouwbaarheid en veiligheid van de onderliggende gegevensverwerking te toetsen. De AVG is niet alleen *lex specialis* maar gaat als EU-verordening boven nationale wetgeving, behoudens situaties waarin Nederland vrije beleidsruimte is gelaten.

Relatie met bestuurlijke verantwoording

Eén van de belangrijkste aspecten van de AVG is bestuurlijke transparantie.⁸ Het college dient op ieder gewenst moment verantwoording te kunnen afleggen over beleid en maatregelen op het gebied van gegevensbescherming – bestuurlijk, maatschappelijk of juridisch.

FG-verslagen helpen het college om de AVG-beleidsvoering geïnformeerd te evalueren, om zo nodig bij te sturen (systeem van ‘checks and balances’). Zolang het college oplossingsgericht besluit in lijn met de AVG, kan de FG dit bevestigen. FG-zienswijzen zijn wettelijk zwaarwegend. Het ligt voor de hand om een en ander te koppelen aan de planning & control-cyclus van de gemeente Edam-Volendam en gegevensbescherming een vaste plek te geven in het jaarverslag.⁹ Voor de accountant is met name de wetenschap van belang dat het college de financiële risico’s beheerst die voortvloeien uit de AVG.¹⁰ Niet in de laatste plaats schept de aanpak goede mogelijkheden om verantwoording af te leggen aan de raad.

⁶ Artikel 37-39 AVG.

⁷ Artikel 38.4 AVG.

⁸ Artikel 5.2 en 24.1 AVG (accountability principe).

⁹ Vgl. *good practices* van bedrijven op dit vlak, mede op basis van de Nederlandse Corporate Governance Code, en de internationale [GRI-standaard voor duurzaamheidsverslaglegging op privacygebied](#).

¹⁰ Met name de financiële risico’s die voortvloeien uit aansprakelijkheid voor individueel geleden schade en de risico’s van last onder dwangsom of bestuurlijke boetes tot 20 miljoen euro.