FG-verslag 2018

Aan: het college van B&W Gemeente Hilversum
Van: mr. S.H. Katus, Functionaris voor Gegevensbescherming

Beoordeling

Gemeente Hilversum trof in 2018 aantoonbaar maatregelen om te voldoen aan de Algemene Verordening Gegevensbescherming (AVG).

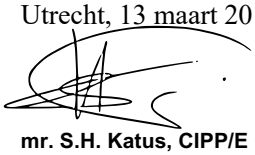
De gemeente is transparant over gegevensverwerking en de bescherming van persoonsgegevens hierbij. Personen hebben toegang tot AVG-dienstverlening zoals het recht op inzage en correctie. Ook kunnen zij contact opnemen met een onafhankelijke functionaris voor gegevensbescherming over alle aangelegenheden in verband met de AVG waarover discussie is ontstaan.

Hiermee is niet gezegd dat Gemeente Hilversum klaar is op AVG-gebied – voor zover dit überhaupt mogelijk is omdat bescherming van persoonsgegevns permanent aandacht en onderhoud behoeft. Voldoen aan de AVG is een complexere uitdaging dan meestal wordt gedacht.

Naar verwachting hebben gemeenten nog zeker drie tot vijf jaar transitie nodig om het kwaliteits- en volwassenheidsniveau te bereiken waar de wetgever vanuit gaat. De uitdaging is om bewust het verband te leggen tussen AVG-voorschriften en behoorlijk gemeentebestuur in het digitale tijdperk.

Gemeente Hilversum verdient vanuit AVG-toezichtperspectief erkenning en vertrouwen dat met de beleidsvoering in dit stadium de juiste richting is gekozen.

Utrecht, 13 maart 2019



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

Privacy Management Partners
Vondellaan 46, 3521 GH Utrecht
E: info@pmpartners.nl
T: 085 401 38 66
W: www.pmpartners.nl

Toelichting

De AVG is niet de technisch-juridische aangelegenheid die er vaak van wordt gemaakt. Inhoudelijk draait de AVG om grip op administratieve processenen en innovatie, en om praktische oplossingen op het gebied van kwaliteit, continuïteit, veiligheid, doelmatigheid en klantgerichtheid (‘mens centraal’).

Om verder te komen, werkt het voor Gemeente Hilversum wellicht het beste om de problematiek te kantelen: focus op procesgericht werken in plaats van voldoen aan de AVG. Maar doe dat dan kaderscheppend, waarbij voorschriften in de AVG randvoorwaardelijk zijn.

Het AVG-werkprogramma en het AVG-ondersteuningsteam staan dan niet op zich maar werken aan de toekomstbestendigheid van de gemeentelijke bedrijfsvoering, in samenwerking met anderen binnen de gemeente zoals risico managers, professionals op het gebied van informatisering & automatisering, documentaire informatievoorziening of bijvoorbeeld degenen die het Smart City Project voeren.

Ontwikkellijn
De ontwikkellijn die hierna wordt weergegeven, geeft aan in welke mate Gemeente Hilversum aan de AVG voldoet. Dit gebeurt aan de hand van de tien belangrijkste toetspunten die logischerwijs uit de AVG voortvloeien. Zie de bijlagen voor nadere toelichting.

De ontwikkellijn is gelaagd. De algemene ontwikkellijn geeft op het hoogste niveau aan hoever de gemeente is. De ontwikkellijn per aandachtsgebied geeft aan hoever de gemeente op dit onderliggende niveau gevorderd is met de AVG-transitie.

De verbinding tussen beide ontwikkellijnen wordt vooral gevormd door punt 5 ‘privacy by design’ en punt 6 ‘ketenregie’ op de algemene ontwikkellijn: hier wordt pas resultaat geboekt wanneer de ontwikkellijn per aandachtgebied daar in de volle breedte voldoende aanleiding toe geeft. Hierbij moet worden opgemerkt dat niet alle aandachtsgebieden even ‘spannend’ zijn: gegevensbescherming in het kader van jeugd en onderwijs weegt bijvoorbeeld zwaarder dan bij cultuur en sport.

Taartgrafieken
Aan de hand van drie taartgrafiekjes wordt per toetspunt 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). Ineffectieve maatregelen dienen vanuit de AVG-regievoering te worden bijgesteld.

Niet onderzocht, afwezig of niet aantoonbaar | In aanzet aanwezig en aantoonbaar | Substantieel aanwezig en aantoonbaar | Grotendeels aanwezig en aantoonbaar | Volledig aanwezig en aantoonbaar

Verantwoording
De FG is onafhankelijk wettelijk toezichthouder op basis van artikel 37-39 AVG. Dit FG-verslag is totstandgekomen op basis van gesprekken met de medewerkers van Gemeente Hilversum en beoordeling van beleidsdocumenten.

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. De accountant beschikt op deze manier over een in onafhankelijkheid afgegeven beoordeling, terwijl het FG-verslag tevens aansluit bij de rechtmatigheidsverant-woording door het college vanaf 2021.

Begrippen
AVG: Algemene Verordening Gegevensbescherming
Bestuurlijk privacybeleid: beleidskader en werkprogramma
BIG: Baseline Informatiebeveiliging Nederlandse Gemeenten
CISO: chief information officer, degene die de gemeentelijke informatiebeveiliging coördineert
FG: functionaris voor gegevensbescherming, wettelijk toezichthouder volgens artikel 37-39 AVG
PIA: privacy impact assessment, de AVG-risicoanalyse die aan een procesplan vooraf gaat
PIT: privacy en informatiebeveiliging team (het AVG-ondersteuningsteam van de gemeente)
PO: privacy officer (degene die de uitvoering van het AVG-beleid coördineert)
Portefeuillehouder: collegelid dat namens het college de AVG-beleidsvoering bewaakt
Procesplan: de documentatie van praktische oplossingen voor de bescherming van persoonsgegevens op operationeel niveau (vervolg op een PIA)
Privacy by design: de implementatie van organisatorische en technische beheersmaatregelen voo de bescherming van persoonsgegevens (vervolg op een procesplan).
Risicoprofiel: waardering van AVG-risico's, voor de duidelijkheid uitgedrukt in PIA-scores variërend tussen 0 en C3.

Ontwikkellijn algemeen

Speerpunten	Opzet	Bestaan	Werking	Advies
1. Beleid				Upgrade het privacybeleid en -reglement naar een SMART en risicogestuurd data protectie management-aanpak ('DPMS'). Formuleer eerst de missie vanuit de eigen visie op gemeentebestuur in het digitale tijdperk, ook vanuit de kernwaarden. Het college is bij wet verantwoordelijk voor sturing (bestuurlijke borging). Zorg daarom voor de verbinding met de planning & control-cylcus.
2. Regie en support				Positioneer duidelijker het AVG-ondersteuningsteam ('PIT') en verbreed deze met andere professionals – desnoods op afroepbasis. Verduidelijk daarnaast dat niet het PIT maar proceseigenaren verantwoordelijk zijn. Het PIT assisteert volgens de 'S' van RASCI.
3. Toezicht				Waarborg dat, naast het FG-toezicht, vooral ook het college en de directie de nakoming van afspraken bewaken. Overweeg het opnemen van een schakelfunctie voor de algemeen directeur in de AVG-beleidsvoering. Waarborg dat de FG-functie kwalitatief goed in gevuld blijft.
4. Werkprogramma				Voer een AVG-risicoanalyse uit op de bedrijfsvoering en bepaal welke aandachtsgebieden in 2019 prioriteit krijgen voor AVG-checkup volgens punten 5 en 6. Neem in het werkprogramma 2019 ook overige actiepunten op die uit dit overzicht voortvloeien. Knip het werkprogramma op in jaarplannen.
5. Privacy by design				Verlang van proceseigenaren dat zij zich een scherp beeld vormen van zowel hun werkprocessen en bijbehorende gegevensverwerking als de intrinsieke risico's hiervan. Zorg met behulp van een 'procesplan-aanpak' dat passende maatregelen worden geeffectueerd om die risico's te beheersen. Op die manier wordt de bescherming van persoonsgegevens operationeel gewaarborgd en voldoet de gemeente 'binnenshuis' aan de AVG.
6. Ketenregie				Zorg in het verlengde van punt 5 tegelijkertijd voor opwaardering van alle vormen van -ketensamenwerking waarbij persoonsgegevens worden gedeeld, zodat de bescherming van persoonsgegevens ook 'buitenshuis' wordt gewaarborgd. Ga niet alleen overmatig data delen tegen maar ook onterecht 'hokjesdenken'.
7. Verzoeken, klachten en incidenten				Breng huidige voorzieningen voor inwoners en medewerkers in overeenstemming met de AVG, een en ander ook volgens een protocol AVG-dienstverlening dat onder meer het recht van toegang tot de FG waarborgt. Richt incidentmanagement zodanig in dat deze slagvaardig is en uit incidenten lessen kunnen worden getrokken. Zorg hierbinnen voor een datalekken-aanpak conform artikel 33 AVG.
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				Stem de informatiebeveiligingsbehoefte af op de procesplanaanpak. In afwachting hiervan valt alvast te voorzien in bijvoorbeeld een infrastuctuur voor *role based access management* en veilige loketten voor verlening van AVG-services volgens punt 7.
10. Budget				Stel een begroting op voor de uitvoering van AVG-werkzaamheden volgens de punten 1 t/m 9. Wijs ook in 2019 de financiële middelen toe die nodig zijn voor AVG-beleidsvoering. Voorzie in ieder geval structureel in budget voor een gekwalificeerde FG (intern of extern), aangezien een FG wettelijk verplicht is.

Ontwikkellijn per aandachtsgebied.

Er heeft nog geen toetsing plaatsgevonden van AVG-nakoming binnen de verschillende aandachtsgebieden

Aandachtsgebied	Opzet	Bestaan	Werking	Advies
1. **Belastingheffing**				Realiseer procesplannen en implementeer maatregelen.
2. **Burgerzaken**				Er worden al langere tijd strenge eisen gesteld aan BRP en BSN, maar nog niet zozeer vanuit de AVG. Hanteer daarom evengoed een procesplan-aanpak.
3. **Cultuur en sport**				Realiseer procesplannen en implementeer maatregelen.
4. **Fraudeonderzoek**				Realiseer procesplannen en implementeer maatregelen. Fraudeonderzoek kan ook onderdeel zijn van andere taakuitoefening (bijvoorbeeld als activiteit binnen werk en inkomen).
5. **Interne organisatie**				Realiseer procesplannen en implementeer maatregelen.
6. **Jeugd en onderwijs**				Realiseer procesplannen en implementeer maatregelen.
7. **Lokale economie**				Realiseer procesplannen en implementeer maatregelen.
8. **Welzijn en zorg**				Realiseer procesplannen en implementeer maatregelen.
9. **Bescherming en opvang**				Realiseer procesplannen en implementeer maatregelen.
10. **Milieu en duurzaamheid**				Realiseer procesplannen en implementeer maatregelen.
11. **Ruimte en bereikbaarheid**				Realiseer procesplannen en implementeer maatregelen.
12. **Veiligheid en openbare orde**				Realiseer procesplannen en implementeer maatregelen.
13. **Werk en inkomen**				Realiseer procesplannen en implementeer maatregelen.

Bijlage I - Beeld stand van zaken na auditgesprekken

Speerpunten	Bevindingen
1. Beleid	De intentie om aan de AVG te voldoen is aanwezig. De vertaling van deze intentie in strategie en tactiek is echter nu nog onvoldoende. Met name ontbreekt nog teveel de risicosturing van artikel 24 e.v. AVG (hierna: 'procesplan-aanpak') voor passende beheersmaatregelen. Goed ging dat het sociaal domein als meest risicovol begrepen werd en prioriteit kreeg. Voor verdere professionalisering is gedegen risico-analyse nodig.
2. Regie & support	De portefeuillehouder in het college zet goede toon. In de transitie van ingehuurde kennis naar een organisatie met eigen personeel is evenwel een gat ontstaan in de overdracht. Hierdoor heeft het team zoals dat waarschijnlijk tot juni heeft bestaan nu niet meer aanwezig. De verdeling van taken en verantwoordelijkheden is hierdoor onvoldoende duidelijk. Er is geen duidelijk aanwijsbaar multidisciplinair team aanwezig. Er zijn wel individuen met goede capaciteiten maar coördinatie ontbreekt nog. Het AVG-ondersteuningsteam heeft zich met name toegelegd op de aanleg van het register van verwerkingsactiviteiten volgens artikel 30 AVG ('verwerkingsregister').
3. Toezicht	Gemeente Hilversum werkt thans samen met een gekwalificeerde FG voor onafhankelijk toezicht (3e lijn). Toezicht/bewaking dient in eerste instantie evenwel uit te gaan van 'iedereen' (1e lijn) – met name proceseigenaren en het college, ondersteund door het PIT (2e lijn). Vanwege punten 1 en 2 is dit nog niet goed vormgegeven.
4. Werkprogramma	Sinds juni ontbreekt een duidelijk jaarplan. De privacy officer legt zich nu nog toe op uitvoering van 1e lijn-ad hoc werkzaamheden. De andere taken zijn diffuus belegd. Het ontbreekt aan een structuur. Zie ook opmerking bij 1-3.
5. Ketenregie	Er is geen duidelijke ketensturing, mede door het ogenschijnlijk ontbreken van een multidisciplinaire aanpak is er geen regievoering op ketens en samenwerkingen. In 1 op 1 verwerkingen (controller/processor) is er sturing (afdeling inkoop is goed betrokken bij proces).
6. Privacy by design	PbD is gesignaleerd als belangrijk. Dit heeft echter nog geen uitwerking gekregen. En zijn nog geen DPIA's uitgevoerd binnen de gemeente. Er zijn wel, geïnitieerd vanuit IB, verbeteringen aangebracht in voor gegevensbescherming kritieke maatregelen (autorisaties).
7. Verzoeken, klachten en incidenten	Geen van de vanuit de AVG verwachte processen zijn als zodanig herkenbaar in opzet aanwezig. Het datalek proces is difuus en heeft een onduidelijke eigenaar, processen rondom rechten van betrokkenen zijn bij de geinterviewde onbekend.
8. Communicatie & training/opleiding	Voor de huidige status van de organisatie, en mede gezien dit rapport voldoende.
9. Informatiebeveiliging	De gemeente werkt met de BIG en doet hierover ook verslag in ENSIA. Ook binnen het IB proces zijn rollen en verantwoordelijkheden diffuus en mogelijk onverenigbaar belegd. De IB organisatie heeft mogelijk vergelijkbare issue's in sturing en uitvoering als de privacy organisatie.
10. Budget	Budget lijkt voldoende. Bij de geinterviewde was niet bekend of er een specifiek budget is geoormerkt voor AVG-beleid.

Bijlage II - 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. Afhankelijk van de taakverdeling binnen een gemeenten zijn dat het college, de burgemeester, de raad en de rekenkamercommissie.[1]

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 Algemeen Rekenkamer luiden inmiddels de noodklok dat hiervan in de praktijk veel te veel voorbeelden zijn.[2] 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* gemeentelijk 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 gemeenten, 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*.[3] 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

---

[1] Kamerstukken 25 892, nr. 3, p. 57. Rekenkamercommissie die niet werkelijk op afstand staan van de raad, zijn geen AVG-verantwoordelijke. Zie ook VNG-handreiking lokale rekenkamer en rekenkamerfunctie.
[2] Zie Rapport Basisregistraties van de Algemene Rekenkamer (2014) en het rapport Zorgen voor Burgers van de Nationale Ombudsman (2018).
[3] 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.

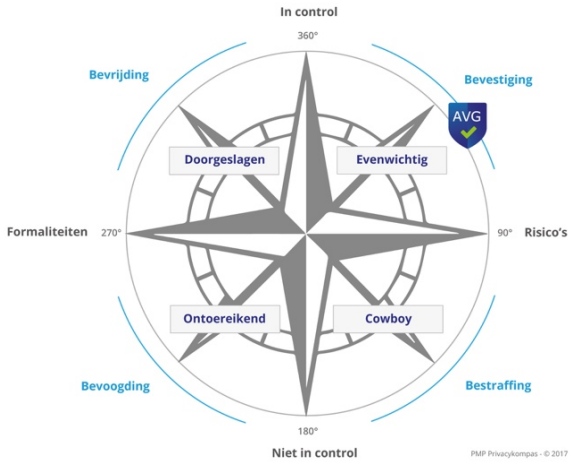
Begrenzing van verantwoordelijkheid

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 dat ook de nieuwe AVG-verantwoordelijke de bescherming van persoonsgegevens op passende wijze waarborgt. Wanneer gegevens eenmaal zijn verstrekt aan derden zoals zorginstellingen, de Politie 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 ‘verwerkinsgsregister’ 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 níet AVG-conform. Om aan de AVG te voldoen is daarmee is 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 te ijken aan de AVG en om de juiste koers aan te houden. Voldoen aan de AVG is altijd ‘rechtsboven’. De lichtblauwe buitenring verwoordt de stijlen van fair toezicht per kwadrant.

10 hoofdkenmerken

Op basis van het voorgaande en aan de hand van 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 artikelen 39-39 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 gegevenseffectbeoordelingen (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. PIA'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 PIA'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.

Bijlage III - 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.[4] 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 evenzeer de taak van de FG om de AP te verduidelijken waarom Hilversum het goed doet ('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.[5] De FG vervult in die gevallen een rol die doet denken aan beroep en bezwaar, zij het op basis van de AVG ('FG-ombudsfunctie'). De klachtencommissie en de algemene gemeentelijk ombudsfunctie beoordelen langs de lijnen van de Algemeen Wet Bestuursrecht de inhoudelijke zorgvuldigheid van gemeentelijk handelen. De FG helpt door de rechtmatigheid, betrouwbaarheid en veiligheid van de onderliggende gegevensverwerking te toetsen.

Relatie met bestuurlijke verantwoording

Eén van de belangrijkste aspecten van de AVG is bestuurlijke transparantie.[6] 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 Gemeente Hilversum en gegevensbescherming een vaste plek te geven in het jaarverslag.[7] Voor de accountant is met name de wetenschap van belang dat het college de financiële risico's beheerst die voortvloeien uit de AVG.[8] Niet in de laatste plaats schept de aanpak goede mogelijkheden om verantwoording af te leggen aan de raad.

---

[4] Artikel 37-39 AVG.
[5] Artikel 38.4 AVG.
[6] Artikel 5.2 en 24.1 AVG (accountability principe).
[7] 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.
[8] 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.