FG-advies

Aan: Het PIT
Van: De functionaris gegevensbescherming
Betreft: Reactie op concept privacybeleid
Datum: 7 november 2024

Graag geef ik advies over tweede concept van een voorstel voor hernieuwd AVG-beleid. Het is positief dat de gemeente hiermee bezig is. Ik verstrekte daarvoor het beleidsmodel Mens Centraal Digitaal. De gemeente heeft de optie om dat beleid op maat te maken. Maar op een andere manier tot oplossingen komen is ook prima – het gaat om het resultaat: beleid dat doet wat het doen moet.

Voor het conceptbeleid is gebruik gemaakt van een beleidsmodel van de IBD. Dat stelt mij voor de opgave om een vergelijking te maken, uitgaande van wat de AVG daadwerkelijk regelt. De kernvraag is: welke dingen moet het bestuur goed vastleggen in een beleidskader – het basisdocument – voor succesvolle realisatie van AVG-doelen?

Om het conceptbeleid te beoordelen, heb ik zeven aspecten op een rij gezet.

1. Visie en missie

Vergelijking of er goede aansluiting is met de beleidsdoelen van de AVG. Op zich mag dat ook uit een ander document blijken waarin de gemeentelijke kernwaarden en toekomststrategie worden gekoppeld aan de AVG-doelen. Maar is dat dan ook échte koppeling? De AVG laat veel ruimte voor flexibiliteit, maar aan de te bereiken resultaten en methodiek valt niet te tornen. Tegelijkertijd ondersteunt de AVG bij échte koppeling de gemeente in haar bedrijfsvoering, taakuitoefening en realisatie van bestuurlijke ambities.

2. Eigenaarschap

Vergelijking van de mate waarin het eigenaarschap goed is geregeld en een integrale aanpak wordt gehanteerd, met ook aandacht voor bestuurlijke mogelijkheden in het digitale tijdperk, zoals het kunnen oplossen van ernstige schuldenproblematiek, woningnood of ondermijning.

3. Tegengaan van administratieve lasten

Is er aandacht voor het bereiken van meer met minder complexiteit en rompslomp?



4. Risicosturing op basis van een bestuurlijke prioritering

Vergelijking van de aandacht voor een bestuurlijk werkprogramma voor realisaties van AVG-doelen over de volle breedte van de gemeentelijke bedrijfsvoering. Je kunt niet alles tegelijk en hebt beperkte middelen, dus hoe kom je tot prioritering?

5. Onafhankelijk Toezicht

Solide afspraken over derde lijn-borging van de beleidsvoering; toegang tot expertise en onafhankelijke toetsing.

6. Behoorlijk bestuur met data

Duidelijke koppeling met behoorlijk bestuur en de Algemene wet bestuursrecht: geen Toeslagenaffaires op Gemeentelijke schaal (de AVG garandeert in essentie je digitale rechtsbescherming). Met name garandeert de AVG zorgvuldige besluitvorming in de zin van 3:2 Awb en de administratieve afhandeling daarvan.[1]

7. Toewerken naar een volwassen cultuur

Het vermogen om AVG-rechtsbescherming te waarborgen onder voortdurend veranderende omstandigheden omdat het in het DNA van de organisatie zit.

Mijn reactie

Het conceptbeleid voldoet grotendeels aan AVG-normen. Als tweede lijn-stuk kan ik het document plaatsen, maar daarmee ligt de nadruk ligt meer op control en informatiebeveiliging dan op behoorlijk bestuur met data.

Bijvoorbeeld: de zin *'Kernpunten (…) zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van(persoons)gegevens. Inwoners, bezoekers, ondernemers, medewerkers en (keten)partners (belanghebbenden) mogen erop vertrouwen dat we passende bescherming bieden bij de verwerking van hun (persoon)gegevens'*, leest als vereenzelvigen van de kernpunten van informatiebeveiliging met de AVG-doelen.

- *Maak de koppeling met lokaal bestuur*

Begrijp de AVG als de omgevingswet voor de digitale leefomgeving. Voer eerste lijn-beleid op aan de hand van een visienota zoals de Omgevingsvisie Hilversum 2040. Dat zou eruit kunnen zien als een mix tussen de concernagenda, iVisie en het herindelingsontwerp.

- *Leg de nadruk op een integrale aanpak*

Versterk eigenaarschap volgens het three lines-model, aan de hand van een integrale aanpak waarbinnen AVG-doelen worden gerealiseerd zonder dat dit 'AVG' hoeft te heten (onbewust bekwaam is ook prima). Bestuur en management, ondersteund door de tweede lijn, hebben teamspel te betrachten voor realisatie van AVG-doelen, ieder vanuit zijn/haar

[1] Vgl. FG-klachtbeoordeling van 29 april 2022 (bestuurlijke informatievoorziening i.v.m. gebiedsverbod).

kracht en competenties. Hiervoor is ook een regiegroep op directieniveau nodig is. Daarnaast; het voorgestelde beleid geeft nog niet het juiste beeld van de normstelling op het gebied van rollen en verantwoordelijkheden volgens de wettelijke eisen (zie hierna).

- *Hanteer een bestuurlijk programma*

DPIA's worden genoemd, maar benadruk dat ze hét instrument zijn voor de ontwikkeling van realistische scenario's waarin inwoners of andere doelgroepen gedupeerd raken door digitalisering. Maak afspraken over bestuurlijke prioritering van risico's en het vinden van oplossingen dat door het directieteam ten uitvoer wordt gelegd (het DT doet de voorstellen). Heb ook oog voor het benutten van nieuwe mogelijkheden – zéker als je daardoor belangrijke maatschappelijke vraagstukken oplost.

- *Verhef eenvoud tot thema*

Er is weinig aandacht voor het tegengaan van onnodige complexiteit en red tape. Stel steeds de vraag of een aanpak of procedure werkelijk bijdraagt aan een mens centrale gemeente. Dit sluit aan bij de bredere doelstellingen van het zijn van een efficiëntere overheid en verbetering van de dienstverlening (menselijke maatvoering).

- *Corrigeer de FG-rol*

Maak solide afspraken over de FG-positie als de derde lijn-toezichthouder op de interne naleving van de AVG in de gemeenteorganisatie op bestuursniveau. Corrigeer wat over de FG geschreven wordt vooral ook aan de hand van de informatie in Wat is een FG?. Maak onder meer de afspraak dat de FG gevraagd wordt om mee te denken bij strategische beslissingen op het gebied van digitalisering en samenwerking met partners. Dit versterkt de waarborg voor naleving van de AVG op lange termijn. Let erop dat de FG ook de toezichthouder is op hoe de gemeente audits organiseert.[2] Althans; voor zover audits AVG-relevantie hebben.

- *Dejuridiseer*

Leg de nadruk op behoorlijk bestuur in het digitale tijdperk. De AVG brengt niet met zich mee dat gemeente wordt opgezadeld met nóg meer wettelijk plichten ('lastig en ingewikkeld'). Maar is de wet op mens centrale digitalisering en ketensamenwerking: hoe doe je dat? Compliance ontstaat vrijwel 'vanzelf' door de goede dingen goed te doen en dat te documenteren, op een transparante manier en in dialoog met doelgroepen (de burger betrekken).[3]

[2] Artikel 39.1b AVG

[3] Artikel 5.1a-b AVG verwoorden het legaliteitsbeginsel, zorgvuldigheidbeginsel en transparantiebeginsel, om vervolgens aan te geven dat verwerking van persoonsgegevens ethische en maatschappelijk wenselijke / ethische en (democratisch) vastgestelde doelen moet dienen. De dialoog vind je terug in artikel 35.9 AVG over DPIA's.

- *Zet in op het bereiken van een volwassen cultuur*

Leg bij PDCA-cyclus en trainingen nog meer de nadruk op doelen, veerkracht bij plotselinge tegenvallers en uitdagingen zoals personeelsverloop, veranderingen in wetgeving, technologische ontwikkelingen en krachten in de samenleving. Goede DPIA's *zijn* trainingen, omdat je met elkaar alle aspecten van een bepaalde werkwijze bespreekt (procesbeschrijving, informatiebehoeften en bewaarplichten, risicoscenario's en logische maatregelen om ongelukken te voorkomen).

- *Relativeer 'strategisch'*

De AVG is inderdaad een strategische wet. Maar verwar basisprincipes in artikel 5 AVG niet met de strategische beleidsdoelen in artikel 1 (waarborgen van rechtsbescherming door middel van bestuurlijke taakstelling / ruimte voor bestuurlijke vernieuwing en informatiedeling).

- *Maak de beleidsvoering zichtbaar in de gemeentebegroting*

Zie aanbevelingen in het FG-verslag 2023-2024.

Het three lines-model in de AVG

Het three lines-model (vroeger: three lines of defense) is gericht op de risicobeheersing via de organisatiestructuur. Het three lines-model ligt ook besloten in de AVG – zij het op een specifieke manier:

- **De eerste lijn** omvat de werkvloer tot en met het bestuur. In de eerste lijn worden de dagelijkse activiteiten uitgevoerd en berust de zeggenschap. De eerste lijn is verantwoordelijk voor het identificeren en beheren van risico's binnen hun eigen processen en activiteiten.[4]
- **De tweede lijn** bestaat uit de staffuncties die de eerste lijn ondersteuning bieden op basis van hun specialisme (ICT, communicatie, juridische zaken, inkoop, risk management, ...). De tweede lijn helpt bij het ontwikkelen van beleid en procedures en zorgt ervoor dat de eerste lijn deze effectief kan implementeren.[5]
- **De derde lijn** is in de AVG de functionaris voor gegevensbescherming. Deze houdt toezicht op interne naleving van de AVG door de organisatie als geheel. Dus ook het bestuur en andere gemeentelijke controlefuncties.[6]

De kerngedachte is dat als de eerste lijn alles goed doet op AVG-gebied alles goed gaat en kansen optimaal worden benut. Tweede lijn-ondersteuning is daarvoor onmisbaar en brengt schaalvoordelen met zich mee (staffuncties ondersteunen meerdere afdelingen).

[4] Artikel 24-31 AVG (Afdeling 1) normeert eigenaarschap in de eerste lijn

[5] Artikel 32-36 AVG (Afdeling 2) veronderstelt ondersteuning in de tweede lijn

[6] Artikel 37-39 AVG (Afdeling 3) definieert het toezicht in de derde lijn

Het FG-toezicht is de *fail safe* (uiteindelijk is er altijd nog de FG),[7] door de doelmatigheid en doeltreffendheid van de aanpak te bewaken (realisatie van AVG-doelen). Op die manier beheers je ook de risico's van afvinkcultuur en overdadige technocratie.[8]

Mijn advies aan het PIT

Zes jaar nadat de AVG is ingevoerd, volstaat het niet meer om te werken op basis van een klein team van privacy officers en informatiebeveiligers.
In het FG-verslag 2022 doe ik daarvoor concrete aanbevelingen – in de eerste plaats: 'Maak het advies Mens Centraal Digitaal u eigen in 2024, op een manier die past bij Gemeente Hilversum'.

De meest gemakkelijke manier om dat te doen, is door overal in de tekst '[Digidam]' te vervangen door 'Gemeente Hilversum'. Gemeente Zeist pakt het zo aan en maakt inmiddels goede vorderingen. Op zich mag het ook helemaal anders, zolang dat maar gebeurt met behoud van functionaliteit en in het verlengde van de gegevensbeschermingswetgeving. Voor mij blijft het dan nog steeds mens centraal genoeg.

Gemeente Hilversum beschikt over een mooie concernagenda. Het modelbeleid Mens Centraal Digitaal kun je hier zo aan ophangen – of beter gezegd; het modelbeleid, als de transponering van de AVG naar gemeentelijke setting, onderstut die concernagenda.

Datzelfde geldt voor het PIT, dat onder de derde iteratie van het beleidskader wel een betere benaming kan gebruiken, maar evengoed belangrijk blijft voor tweede lijn-ondersteuning die typisch AVG zijn. Kernactiviteiten blijven dan ondersteuning op het gebied van artikel 32- en 35-werkzaamheden, dus informatiebeveiliging en DPIA's. Het blijft nuttig om input te leveren voor het werkprogramma en in dat verband voortgangsrapportages te verzorgen.

Routekaart

Maar dit alles meer in samenspel. Stappen 1 en 2 van een DPIA kunnen bijvoorbeeld beter worden gedaan door de collega's die zijn gespecialiseerd in procesinrichting, ICT en informatievoorziening. Stappen 3 en 4 zijn stakeholderoverleg (afdeling communicatie?) om te begrijpen waar de kwetsbaarheden zitten, om zo te komen tot passende mitigerende maatregelen (risico management in de publieke sector). Zó realiseer je dataprotectie by design – ook in ketenverband, wat op uitvoeringsniveau hét resultaat is dat dient te worden gerealiseerd.[9]

[7] 'Hoeksteen van verantwoording' volgens de EU Data Protection Board FG Richtlijnen

[8] Vgl. managementboek Verdraaide organisaties

[9] Artikel 25 AVG

Een en ander althans in **opzet** (vandaar 'design'). Belangrijker is het **bestaan** van die maatregelen. Tijdens een goede DPIA kan blijken dat de gemeente al veel zaken op orde heeft, of dat het hooguit zo is dat enkele aspecten verbetering behoeven. Artikel 35.11 AVG bepaalt met zoveel woorden dat eerste lijn-verantwoordelijken ('proceseigenaren') zo nodig 'bestaan' laten toetsen. Bij de DPIA-begeleiding doe je dat al tot op zekere hoogte. Maar bij een hoger risicoprofiel is er beslist een *business case* voor échte interne of externe audits.

Wat dit laatste betreft; zie artikel 42-43 over AVG-certificering – die de gemeente vanuit de eerste lijn kan organiseren en, als het goed is, ook FG-toezicht ondersteunt. Een en ander dan niet op basis van een generiek auditschema zoals de Wpg-audits (over red tape gesproken), maar op basis van de KPI's die uit DPIA's voortkomen. Dus doelmatig en doeltreffend.

Kortom:
1. Een DPIA is een dialoog;
2. die resulteert in een handboek voor de proceseigenaar (zó doe je het goed);
3. waaruit zinnige KPI's blijken (kwaliteitskenmerken / toetsingscriteria) die in de praktijk moeten worden of zijn gebracht (wat zo nodig wordt getoetst);
4. en de proceseigenaar inzicht en overzicht biedt voor beheer, onderhoud, incident management en change management.

De managementsamenvatting van handboeken verzamelt de gemeente in een centraal overzicht voor sturing en verantwoording ('verwerkingsregister').[10] Bij organisatieveranderingen is er het handboek voor de borging van kwaliteit en continuïteit (ze mogen nooit 'verwezen'). Zolang incidenten uitblijven, blijkt ook de goede **werking**.

Voorkomen is altijd beter dan genezen, dus periodiek hou je handboeken kritisch tegen het licht aan de hand van vervolg-DPIA's. Zo blijft procesoptimalisatie (naleving AVG) een continu proces, zowel incidenteel als structureel (lerende organisatie).

Bewaking vanuit de tweede lijn heeft meer het karakter van begeleiding / ondersteuning. Tooling van GRC-aanbieders kan daarvoor handig zijn, maar gebruik het dan wel voor de hiervoor vermelde stappen – dus óók doelmatig en doeltreffend. In feite is dat dan work flow management, voortgangsbewaking en documentatiebeheer.

[10] Artikel 30 AVG

Denk in dit verband ook aan de administratieve aspecten van:

- deelname in samenwerkingsverbanden;[11]
- regievoering op uitbesteding;[12]
- incident management.[13]

> Het verwerkingsregister vullen aan de hand van data-inventarisaties, kost in de regel veel tijd en energie, en blijft ondoelmatig zolang het niet de overzichtskaart oplevert die bestuurlijke regievoering op digitalisering mogelijk maakt. Het verwerkingsregister is in ieder geval geen doel op zich; je bent niet 'compliant' met de AVG *omdat* je een verwerkingsregister hebt.

Resultaat

Zoals aangegeven; het beleidskader is de basis van dit alles.[14]

A. Gemeente Hilversum digitaliseert volgens de hiervoor aangegeven routekaart conform de doelen en beginselen van de AVG;[15]
B. Waardoor het is het gemeentebestuur op ieder gewenst moment kan voldoen aan haar verantwoordingsplicht;[16]
C. Zodat inwoners, medewerkers en andere doelgroepen verzekerd zijn van bescherming tegen de keerzijden van digitalisering (recht op gegevensbescherming).[17]

PM

1. AVG-dienstverlening rechten van betrokkenen en FG-ombudsfunctie;[18]
2. Internationaal gegevensverkeer bij digitalisering op basis van ICT-dienstverlening buiten de EER;[19]
3. Algoritmes en kunstmatige intelligentie;[20]
4. Overige relevante EU-wetgeving;[21]
5. Nadere uitwerking van EU-wetgeving in Nederlandse wet- en regelgeving;
6. Conflicten in Nederlandse wet- en regelgeving met EU-wetgeving.[22]

[11] Artikel 26 AVG. Zie ook FG-advies van 4 oktober 2023 ([Participatie in een samenwerkingsverband])

[12] Artikel 28 AVG

[13] Artikel 33.5 AVG

[14] Artikel 24.2 AVG

[15] Artikel 24.1 AVG

[16] Artikel 5.2 AVG

[17] Artikel 1 AVG

[18] Artikel 12-22 en 38.4 AVG

[19] Artikel 44-46 AVG

[20] Artikel 22 AVG; EU-verordening Artificiële Intelligentie

[21] EU-wetgeving op het gebied van o.m. open data, elektronische identificatie, ePrivacy

[22] Bij conflict prevaleert het recht van de Europese Unie.

AVG-management als continu proces

(…)

Beschrijf AVG-management als een continu proces en in managementtaal, met inbegrip van een duidelijke risicodefinitie en de methodieken om AVG-kwaliteit doeltreffend en doelmatig te waarborgen, zonder doel en middelen te verwarren.

Om dit concreter te maken: de AVG verplicht nergens tot het sluiten van verwerkersovereenkomsten. Maar uit een deugdelijke DPIA kan blijken dat gestuurd moet worden op harde garanties bij uitbesteding van taken en informatievoorzieningen (KPI's).

Uitbesteding kan een kwestie van inkoop zijn, maar vergeet ook deelname in een gemeenschappelijke regeling niet.[23] De KPI's zijn de in de AVG bedoelde verwerkersafspraken, waaronder concrete eisen op het gebied van informatieveiligheid.[24]

Dat betekent dat 'verwerkersafspraken' niet iets is dat informatiebeveiligers aan de privacy officers kunnen overlaten, zoals op 5 november werd aangegeven, maar dat juist hier samenspel vereist is (integrale aanpak).[25] Bijkomstig voordeel van een deugdelijke DPIA is dat je met elkaar al in dialoog bent – dus het goede gesprek voert.

Het beleidsmodel Mens Centraal Digitaal beschrijft dat je uit een DPIA tevens de AVG-risicoscore volgens de Schaal van Erg hebt te destilleren.[26] Die AVG-risicoscore stelt vervolgens in staat om ook voor het AVG-deelaspect informatieveiligheid, in passende oplossingen te voorzien (welk pakket aan maatregelen is hier concreet vereist – dus opnieuw; de KPI's).[27]

Een en ander aan de hand van deze onderstaande tabel.

	AVG-risicoscore (Waarden 0-C3 volgens de 10-puntschaal Schaal van Erg)				
IV-risico	**Beschikbaarheid**	**Integriteit**	**Vertrouwelijkheid**	**Weerbaarheid**	**Responsiviteit**
Nihil	0	0	0	0	0
Laag	1	1	1	1	1
Midden	2	2	2	2	2
Hoog	3	3	3	3	3

[23] FG-advies van 4 oktober 2023 ([Participatie in een samenwerkingsverband])

[24] Artikel 28.3 AVG

[25] De Cyberbeveiligingswet als uitvoeringswet van zowel de EU NIS2-richtlijn als de AVG en de Richtlijn Justitiegegevens

[26] Beleidsmodel Mens Centraal Digitaal, p. 27

[27] Naleving artikel 32-34 AVG

Integraal risicogestuurd werken
Bijvoorbeeld: als de AVG-risicoscore '0' is, speelt het thema mens centraal digitaal niet (de AVG is niet van toepassing). Je hoeft niet eens aan een DPIA te beginnen. Het beleidsmodel Mens Centraal Digitaal bevat een quick scan om dat AVG-conform kunnen vaststellen.[28]

Terwijl C-waarde op de Schaal van Erg juist kan corresponderen met – opnieuw als voorbeeld – een Responsiviteit 3-score, wat weer correspondeert met de informatieplicht van artikel 34 AVG. Hierop voorbereid zijn, betekent dat één van de uitkomsten van de DPIA is dat de KPI 'crisiscommunicatieplan' passend is.[29] In het kader van een integrale aanpak, is daarvoor samenwerking met de afdeling communicatie nodig.

Maar je bent nergens zonder snelle signalering van incidenten en CERT-achtige afhandeling van zo'n signaal. Als de procesbeschrijving (immers eveneens een product uit de DPIA) uitbesteding aan uitvoeringsorganisaties omvat, is er via de verwerkersafspraken Responsiviteit 3-score, dus ook een 'hoge urgentie-signaleringsprotocol' nodig, en gemeente-interne protocolafspraken over onmiddellijke melding bij de AP door de eerste lijn-verantwoordelijke (proceseigenaar), die daarvoor de ondersteuning krijgt vanuit het PIT.

Bij Responsiviteit 3 ligt het ook voor de hand dat in het handboek (p. 6) afspraken worden gemaakt over calamiteitenoefeningen. Wellicht ontstaan daaruit nieuwe inzichten, die weer helpen in de procesoptimalisatie volgens de Doorontwikkeling ('lerende organisatie').

Naleving AVG
De C-scoring op de Schaal van Erg waar deze voorbeelden van zijn afgeleid, zou bijvoorbeeld een C2-score kunnen zijn, en waarvan de doorvertaling naar informatiebeveiliging in het PIT wordt vastgesteld op BIVWR-score 1.3.1.2.3.

Naast passende oplossingen op het gebied van Responsiviteit, zijn er dus ook nog andere oplossingen nodig die moeten matchen met deze score. Tegelijk blijkt ook dat lang niet alles even zwaar hoeft te worden aangezet – en dat scheelt in de inspanningen en kosten.

AVG-naleving is proces-maatwerk. Hoe hoger de scoring op de Schaal van Erg, hoe meer voorkomen te verkiezen is boven genezen. Concrete oplossingen in het handboek zijn gedeeltelijk tactisch (regievoering), maar vooral ook operationeel (praktische organisatorische en technische oplossingen).

[28] Verbeterde pre-DPIA (vgl. de 'twee vinkjes pre-DPIA' die in de praktijk vaak wordt gehanteerd)

[29] Vgl. crisiscommunicatie Hof van Twente 2020 en de Politie-hack 2024

Informatiebeveiliging is dan nog maar één van de tien AVG-kernpunten. Ook voor de overige 90% zijn passende oplossingen nodig; bestuurlijk, managementmatig en op het niveau van de informatievoorzieningen. Die andere 90% waarborgt des te meer de bestuurlijke integriteit van een aanpak (behoorlijk bestuur en goed werkgeverschap in de datamaatschappij).