venlo

MONITORING EN VERANTWOORDING IN HET KADER VAN BESCHERMING VAN PERSOONSGEGEVENS

DATUM: 25 OKTOBER 2022
VERSIE: 1.0

INHOUDSOPGAVE

1. INLEIDING 3

2. FUNCTIES EN ROLLEN 3

3. TOETSINGSKADER EN DIEPGANG VAN ONDERZOEKEN 6

3.1. INLEIDING 6

3.2. TOETSINGSKADER 6

3.3. AMBITIENIVEAU 7

4. INVULLING VAN DE TOEZICHTHOUDENDE TAAK DOOR DE FG 9

4.1. INLEIDING 9

4.2. DE METHODIEK VAN ONDERZOEK 9

4.3. HET PROCES VAN ONDERZOEK EN VERANTWOORDING 10

4.4. KWALITEIT VAN DOOR DE FG UITGEVOERDE ONDERZOEKEN 10

5. RAPPORTAGES 11

5.1. INLEIDING 11

5.2. RAPPORTAGES DIE GERICHT ZIJN AAN DE GEMEENTERAAD 11

5.3. RAPPORTAGES DIE GERICHT ZIJN AAN COLLEGE, BURGEMEESTER, MANAGEMENT EN FG 12

Bijlage 1: AVG Borgingsproduct versie 2.0 13

Bijlage 2: Handreiking AVG borgingsproduct 2.0 13

Bijlage 3: FG Jaarrapportage model gemeenteraad 13

Bijlage 4: FG Jaarrapportage model college en burgemeester 13

1. INLEIDING

Eén van de belangrijkste verplichtingen die opgenomen is in de Algemene Verordening Gegevensbescherming (AVG) is de verantwoordingsplicht: de gemeente moet kunnen laten zien dat zij aan privacywetgeving en -beleid voldoet. In dit monitorings- en verantwoordingsplan is vastgelegd hoe het college van burgemeester en wethouders (het college) en de directie hier invulling aan geven.

Monitoring en verantwoording in het kader van (privacy) risico's die de organisatie loopt wordt geborgd binnen de reguliere control cyclus. In hoofdstuk 2 en 3 worden de kaders hiervoor gegeven. Hierbij wordt aandacht besteed aan de wijze waarop functies en rollen zijn ingeregeld, het toetsingskader dat wordt gebruikt, en de diepgang van te verrichten onderzoeken.

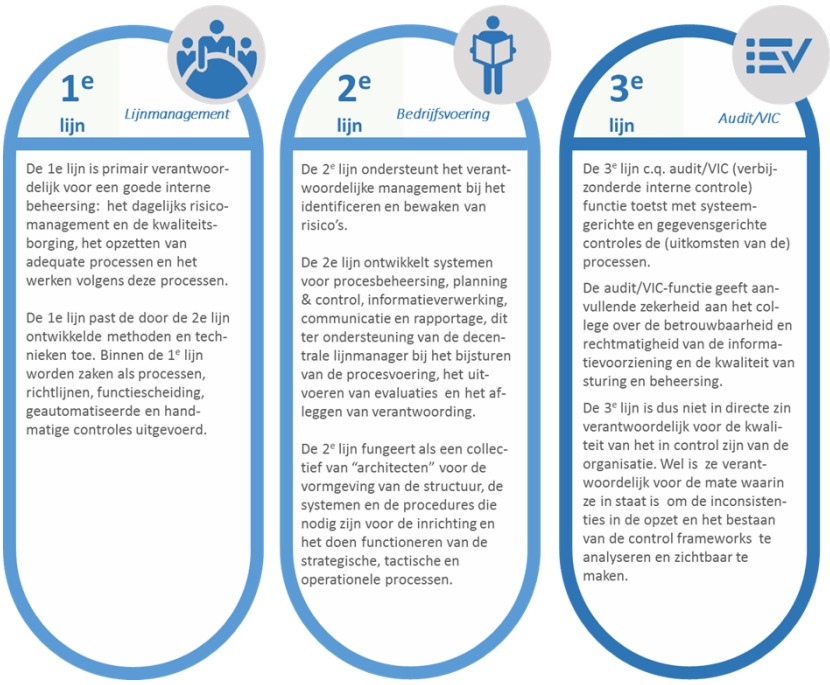
Op grond van de AVG is daarnaast een Functionaris Gegevensbescherming (FG) aangewezen die onafhankelijk toezicht houdt op de toepassing en naleving van privacywetgeving en -beleid. In hoofdstuk 4 wordt toegelicht hoe de FG invulling zal geven aan deze toezichthoudende taak. Hierbij komen de methodiek van onderzoek door de FG, het proces van onderzoek en verantwoording en de kwaliteit van de door de FG uitgevoerde onderzoeken aan de orde.

In hoofdstuk 5 wordt tenslotte aandacht besteed aan de wijze waarop verantwoording plaatsvindt en wordt aangegeven welke rapportages in dit kader uitgebracht zullen worden.

2. FUNCTIES EN ROLLEN

De functies en rollen die van belang zijn voor monitoring en verantwoording in het kader van de bescherming van persoonsgegevens worden nader beschreven in dit hoofdstuk. De gemeente Venlo gaat uit van het zogenaamde Three Lines of Defence model, zoals dat is opgenomen en uitgewerkt in het directiebesluit Control op Informatie[1]. In onderstaande afbeelding worden de taken en verantwoordelijkheden van de 3 (interne) lijnen samengevat:

[1] Zie Onegov zaaknummer 1511342



De rollen en functies die bij de 3 lijnen horen zijn reeds ingevuld bij het directiebesluit 'Control op informatie', met uitzondering van de rol toetser in de tweede lijn. Daarin wordt nu voorzien. Er wordt gekozen voor de privacy officer voor deze taak. Door invulling van de rol toetser in de tweede lijn zien de three lines of defense er als volgt uit:

Beleidsterrein	**1e-lijn**	**2e-lijn (Inrichten)**	**2e-lijn (Toetsen)**	**3e-lijn**
Privacy	Proceseigenaar	Privacy Officer	**Privacy Officer**	VIC / FG

De genoemde functies en rollen hebben de volgende taken[2]:

<u>1e lijn</u>
Proceseigenaar[3]:

- Het formuleren van het doel (outcome) van het werkproces, de wensen van de klant(en) en het definiëren van de output van het werkproces.
- Op regelmatige basis in gesprek met de klant van het werkproces om te bepalen wat de kwaliteit is van de uitvoering van het werkproces.
- Het pro-actief verzorgen van de juiste communicatie naar stakeholders in en rondom het werkproces.
- Doet het werkproces wat het moet doen? Permanente monitoring van prestaties / indicatoren.
- Zorgen dat het procesmodel altijd 'in de pas' loopt met de werkelijke uitvoering; dus de procesbeschrijving up-to-date is.
- Raakvlakken met andere werkprocessen in de gaten houden, ook in het kader van aankomende projecten en IT vernieuwingen.
- Op regelmatige basis het werkproces evalueren met betrokkenen in en rondom het proces.
- Aankomende ontwikkelingen, projecten of systeemvernieuwingen in de gaten houden. Wat is de impact op het werkproces? Hoe moet hiermee om worden gegaan?
- Werking van de beheersmaatregelen toetsen; Eventueel bijstellen van het werkproces op basis van deze toetsing.
- In actie komen als er zich in het werkproces een issue voordoet.

[2] Dit is vastgesteld bij het directiebesluit Control op informatie (zie zaaknummer 1511342)

[3] De taken die bij de rol Proceseigenaar zijn vermeld, zijn al eerder vastgesteld door de directie (zie zaaknummer 1384796).

2e lijn inrichten

Privacy Officer:

- Rollen en verantwoordelijkheden definiëren
- Voorzien in risicobeheersingsmethodiek (gereedschap voor het managen van de risico's door 1e lijn)
- Adviseren in het toepassen van de methodiek van de 1e lijn om processen en controles te ontwikkelen voor risicobeheersing
- Attenderen van de 1e lijn op veranderend beleid of risico's
- Rapporteren aan het management
- Signaleert afwijkingen in de uitvoering ten opzichte van de inrichting naar de proceseigenaar.
- Informeert de kwaliteitsadviseur informatievoorziening en de 3e lijn control bij het uitvoeren van audits

2e lijn toetsen

Privacy Officer:

- Toetsen op de verantwoordelijkheden van de 1e lijn
- Monitoren van de administratieve verwerking:
  - Het effect van de interne controle
  - Nauwkeurigheid en volledigheid van de rapportage van de 1e lijn
  - Conformiteit (compliancy) met wetgeving en regelgeving
  - Tijdig reageren op afwijkingen
- Het monitoren van de implementatie en het toepassen van risicobeheersingsprocessen door de 1e lijn
- Rapporteren aan het management en informeren van 3e lijn control

3e lijn (verbijzonderde interne controle)

Functionaris gegevensbescherming (FG) / Adviseur VIC:

- Toetst het toetsingsproces
- Toetst de interne controles die door de eerste en tweede lijn zijn uitgevoerd
- Rapporteert aan directie

De taken van een hoofd als 1e lijns control blijven ongewijzigd ten opzichte van het eerder vastgestelde kader.

Ook de taken van de privacy officer als 2e lijns inrichter worden niet gewijzigd.

Door aanwijzing van de privacy officer als 2e lijns toetser wordt aangesloten bij de reguliere PDCA-cyclus van de gemeente Venlo. De privacy officer monitort de (her)inrichting van processen conform privacywetgeving. In de teamplannen worden de aandachtspunten voor een team met betrekking tot privacy opgenomen. Deze zijn gebaseerd op het AVG Borgingsproduct[4] als toetsingskader. De businesscontroller monitort de voortgang van de teamplannen middels verantwoordingsgesprekken met de hoofden, en wordt voor de aspecten die betrekking hebben op privacy gevoed door de privacy officer.

Als 3e lijns controller ziet de Verbijzonderde Interne Controle (VIC) toe op het control proces in de eerste en tweede lijn en rapporteert hierover, in het kader van toezicht op bescherming van persoonsgegevens, aan de directie en aan de FG[5].In termen van de *Lines of defence* kan de FG geen onderdeel zijn van de operationele toetsing en is hij daarom eveneens als *third line of defence* gepositioneerd. De FG voert conform het directiebesluit Control op Informatie audits uit en rapporteert aan directie, college, burgemeester en raad over de naleving van privacywetgeving en -beleid.

[4] Zie paragraaf 3.2.

[5] Zie artikel 38 lid1 AVG

In het privacy beleidskader[6] is besloten dat het directieteam verantwoordelijk is voor de integrale sturing van de ambtelijke organisatie op naleving van privacywetgeving en -beleid. De gemeentesecretaris is aangewezen als portefeuillehouder privacy op directieniveau. Hij legt verantwoording af aan het college over het gevoerde privacybeleid, en wordt daarvoor gevoed door de 3 *lines of defence* via overleggen en rapportages.

3. TOETSINGSKADER EN DIEPGANG VAN ONDERZOEKEN

3.1. INLEIDING

Om te kunnen voldoen aan de verantwoordingsplicht wordt een cyclisch proces ingericht , waarbij (door de in hoofdstuk 2 benoemde functies en rollen) gebruik gemaakt wordt van een standaard toetsingskader. Een toetsingskader is opgebouwd uit een verzameling beheersingsdoelstellingen met daarop afgestemde beheersmaatregelen, die in samenhang een kader vormen voor de verwerking van persoonsgegevens en het toezicht daarop. Naast de keuze voor een toetsingskader dient ook besloten te worden met welke diepgang toetsing plaats dient te vinden. Dit wordt bepaald aan de hand van het ambitieniveau van een organisatie.

3.2. TOETSINGSKADER

Het toetsingskader waar in deze uitwerking voor gekozen wordt, is het AVG Borgingsproduct van de VNG/IBD (hierna: “borgingsproduct”). Dit instrument is een algemeen aanvaard toetsingskader dat zich specifiek richt op gemeenten. Door het borgingsproduct toe te passen worden alle aspecten van de AVG belicht en kan inzicht worden gegeven in de mate waarin voldaan wordt aan privacywetgeving en -beleid.
Het borgingsproduct is onderverdeeld in zeven verschillende thema’s waaraan aandacht besteed moet worden om te kunnen voldoen aan de AVG. Het betreft de volgende onderdelen:

- Beleid;
- Organisatorische inbedding;
- Processen;
- Rechten van betrokkenen;
- Samenwerking;
- Beveiliging;
- Verantwoording.

Om te kunnen toetsen in hoeverre de gemeente op de genoemde 7 thema’s voldoet aan privacywetgeving zijn er per thema onderzoeksvragen geformuleerd.

Bij beantwoording van de onderzoeksvragen kan gekozen worden uit verschillende antwoorden die ingedeeld zijn in vijf privacy volwassenheidsniveaus, waarvan niveau 5

[6] Vastgesteld door het college op 11-06-2019, door de burgemeester op 18-06-2019 en de gemeenteraad op 11-09-2019.

het hoogst haalbare is. Per niveau is aangegeven welke maatregelen genomen moeten zijn om aan het betreffende volwassenheidsniveau te voldoen.

Dit ziet er als volgt uit als bijvoorbeeld gekeken wordt naar het thema beleid:

Er is algemeen privacybeleid en uitwerkingen daarvan.	1	Het privacybeleid is niet compleet of bestaat meer informeel. Uitwerkingen van het privacybeleid, bijvoorbeeld een privacyreglement, bestaan niet of nauwelijks.	
	2	Privacybeleid en uitwerkingen daarvan bestaan, maar ze zijn onvolledig en/of alleen bekend bij enkele individuen in de organisatie. Reviews om ervoor te zorgen dat deze documentatie in overeenstemming is met wet- en regelgeving en doelstellingen van de gemeente vinden willekeurig plaats.	Er is een privacybeleid voor de gehele gemeente waarin wordt uitgelegd hoe de gemeente omgaat met persoonsgegevens en hoe de rollen, taken en verantwoordelijken zijn belegd, bij voorkeur vastgelegd in een matrix.
	3	Het privacybeleid en uitwerkingen daarvan zijn compleet, organisatiebreed bekend en makkelijk te begrijpen. Dit draagt bij aan een uniforme benadering van privacy gemeentebreed.	Het privacybeleid is juridisch getoetst en goedgekeurd
			Het privacybeleid is vastgesteld door het verantwoordelijke bestuursorgaan.
			(Wijzigingen in) het privacybeleid is bekend binnen en buiten de organisatie. Communicatiemiddelen worden hiervoor ingezet, zoals intranet, lunchbijeenkomsten en cursussen.
			Er is – waar nodig – domeinspecifiek privacybeleid waarin wordt beschreven hoe het betreffende domein omgaat met (sectorspecifieke) wet- en regelgeving voor zover het gaat om de bescherming van persoonsgegevens.
			Het beschermen van persoonsgegevens is geïncorporeerd in beleidsstukken van andere relevante discipines binnen de gemeente, zoals informatiebeveiliging.
			Eerdere versies van privacybeleidsdocumenten worden bewaard volgens een vastgesteld bewaarschema.
	4	De actualiteit en kwaliteit van het privacybeleid en uitwerkingen daarvan worden periodiek geëvalueerd en het resultaat daarvan wordt gebruikt om deze documentatie te verbeteren. Veranderde wet- en regelgeving en doelstellingen van de gemeente vormen hier een onderdeel van. Dit proces maakt onderdeel uit van een PDCA-cyclus.	Het privacybeleid wordt in de PDCA cyclus in ieder geval elke 3 jaar herzien.
	5	Medewerkers en management houden continu rekening met privacy. Er zijn effectieve procedures die borgen dat wijzigingen en initiatieven die niet voldoen aan het privacybeleid en uitwerkingen daarvan tijdig worden geïdentificeerd en opgepakt. Gesignaleerde tekortkomingen en kansen worden door hen gecommuniceerd	Het privacybeleid is door het management bekrachtigd en wordt actief uitgedragen.

(In de eerste kolom is de onderzoeksvraag opgenomen, in de tweede kolom het volwassenheidsniveau, in de derde kolom een toelichting op het volwassenheidsniveau en in de vierde kolom de maatregelen die genomen moeten zijn om aan een volwassenheidsniveau te voldoen)

In bijlage 1 is de volledige actuele versie (2.0) van het borgingsproduct opgenomen en in bijlage 2 de bijbehorende handreiking.

3.3. AMBITIENIVEAU

Door middel van een 0-meting kan het huidige volwassenheidsniveau van de organisatie bepaald worden. De nulmeting is opgenomen in de auditplanning van de FG. Naast bepaling van het huidige volwassenheidsniveau van de gemeente Venlo is het van belang om voor de komende jaren het ambitieniveau vast te stellen, zodat hierop binnen de planning en controlcyclus gestuurd kan worden.

De vijf volwassenheidsniveaus die gehanteerd worden in het borgingsproduct, zien er als volgt uit:

1	Ad hoc	• Geen of onduidelijke privacyrollen en -verantwoordelijkheden • Geen of nauwelijks beheersmaatregelen aanwezig • Reactief en sturing n.a.v. incidenten • Grote afhankelijkheid van één of enkele privacyfunctionarissen • Onbewust onbekwaam
2	Herhaalbaar	• Privacyrollen en -verantwoordelijkheden toegewezen • Beheersmaatregelen zijn aanwezig, maar worden op informele wijze uitgevoerd • Standaarden en formats aanwezig: juist en in duidelijke taal • Bewust onbekwaam
3	Bepaald	• (Privacy)medewerkers tonen eigenaarschap, d.w.z. dat de rollen en verantwoordelijkheden actief worden opgepakt • Er wordt aantoonbaar aan verplichtingen voldaan • Verwerkingsverantwoordelijke bestuursorganen nemen beslissingen mede op grond van risicoanalyses zoals een DPIA. • Er is een duidelijke samenhang met informatiebeveiliging • Bewust bekwaam
4	Beheerst	• De effectiviteit van beheersmaatregelen wordt periodiek geëvalueerd in een PDCA-cyclus • Er wordt proactief geïnformeerd door de proceseigenaar over de realisering van de geconstateerde benodigde verbeteringen in een PDCA-cyclus • In een jaarlijkse evaluatie blijkt een correcte PDCA-cyclus • Bewust bekwaam
5	Geoptimaliseerd	• Toekomstgericht • Proactieve houding van het college en het bestuur • Het verantwoordelijk management verzoekt aan de FG om hun verantwoording van een oordeel te voorzien. • Privacy wordt gezien als een vanzelfsprekendheid • Er wordt continue gezocht naar verbetering, zoals in de vorm van (interne of externe) tooling • Privacy wordt gezien als een kans of unique selling point (USP) • Er wordt verbinding gezocht met andere concerndisciplines • Kennis en ervaringen worden actief gedeeld met gemeenten en andere relevante organisaties waardoor best practices in gemeentenland ontstaan • Onbewust bekwaam

Alom wordt erkend dat niveau 3 noodzakelijk is om aan wet- en regelgeving te voldoen. In het privacy beleidskader heeft de gemeente Venlo een duidelijke missie, visie en ambitie voor (in ieder geval) de komende jaren geformuleerd:

> "*De gemeente Venlo ziet bescherming van persoonsgegevens als een zaak van behoorlijk bestuur. Inwoners en medewerkers moeten erop kunnen vertrouwen dat persoonsgegevens rechtmatig, zorgvuldig en veilig worden verwerkt. De bestuursorganen zorgen daarom voor de randvoorwaarden van een privacy bewuste organisatiecultuur en voeren in dat kader een adequaat privacy beleid. Zij zijn transparant over hun gegevensverwerkingen en de manier waarop deze gegevens worden beschermd. Zij zorgen voor een goede balans tussen adequate bescherming van privacy en effectieve processen om betrokkenen te bedienen*".

Hiermee heeft de organisatie gekozen voor een volwassenheidsniveau op in ieder geval niveau 3. Dat is ook het ambitieniveau waarvoor gekozen wordt in dit plan.

4. INVULLING VAN DE TOEZICHTHOUDENDE TAAK DOOR DE FG

4.1. INLEIDING

Zoals in de voorgaande hoofdstukken toegelicht geeft de reguliere planning en control cyclus inzicht in de manier waarop de gemeente haar doelstellingen op privacy gebied bereikt.
De door de gemeente aangestelde FG (de functionaris die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG[7]) staat vanuit een onafhankelijke positie de bestuursorganen bij door toezicht te houden op de interne naleving van de AVG[8]. De werkzaamheden die de FG vanuit zijn toezichthoudende functie verricht zijn aanvullend op de monitoring- en verantwoording zoals die plaatsvindt binnen de reguliere planning en control cyclus.

Nu gaandeweg naar een fase toegegroeid wordt waarin de basisimplementaties afgerond zijn, is het van belang dat de werkzaamheden van de FG gelijke tred houden met deze ontwikkeling. Dit vereist een grotere nadruk op toezicht. In dit hoofdstuk zal toegelicht worden welke methodiek de FG gebruikt bij het doen van onderzoek, hoe de kwaliteit van de door de FG uitgevoerde onderzoeken geborgd wordt en hoe het proces van onderzoek en verantwoording eruit ziet.

4.2. DE METHODIEK VAN ONDERZOEK

Er is nog geen algemeen aanvaarde onderzoeksmethode voor het houden van toezicht door de FG. Er wordt daarom voor gekozen om zoveel als mogelijk aansluiting te zoeken bij de binnen de accountancy gehanteerde methode van procesgericht onderzoeken. Een dergelijk onderzoek kent drie fasen; te weten het beoordelen van opzet, bestaan en de werking van een proces.

A) **Beoordeling van de opzet:** dit is de beoordeling of er voor een bestaand proces of project beleid, of andersoortige kaders zoals bijvoorbeeld een projectplan of businesscase, ontworpen en vastgesteld zijn en of binnen die kaders alle noodzakelijke maatregelen zijn opgenomen om te kunnen voldoen aan privacy wet- en regelgeving.

B) **Beoordeling van het bestaan:** onderzocht wordt of de kaders (zoals aangetroffen bij de beoordeling van de opzet) vertaald zijn naar procedures, activiteiten en concrete maatregelen/gedrag in de praktijk. In geval van een projectbeoordeling wordt gekeken naar voortgangsverslagen, probleemregistraties, test en opleveringsverslagen en dergelijke. Deze beoordeling vertelt iets over ‘hoe’ het proces of project er op privacy gebied voor staat qua voortgang en beheersing.

C) **Beoordeling van de werking:** bij de beoordeling van de werking wordt vastgesteld of de procedures en (beheers)maatregelen effectief zijn. Een voorbeeld is een periodieke controle op loggegevens om vast te stellen of

[7] Artikel 39 lid 1 onder b AVG
[8] Overweging 97 AVG

medewerkers alleen toegang hebben tot die gegevens die zij voor hun werkzaamheden nodig hebben.

De omvang van de beoordeling zal per onderzoek worden bepaald, waarbij het uitgangspunt is om de spreiding van de te onderzoeken massa over de onderzoeksperiode evenredig te verdelen. Indien er geen procesgerichte benadering mogelijk is dan zal met een steekproef of deelwaarneming worden gewerkt.

4.3. HET PROCES VAN ONDERZOEK EN VERANTWOORDING

In deze paragraaf wordt kort het proces van het onderzoek door de FG en de verantwoording daarover weergegeven. Er zijn twee uitgangspunten bij het doen van onderzoek en verantwoording: transparantie en het voorkomen dat lopende onderzoeken van anderen worden doorkruist of dubbel worden uitgevoerd. Deze uitgangspunten vormen de basis voor een jaarlijks door de FG op te stellen auditplanning. In afwijking van de auditplanning kan het voorkomen dat nader onderzoek nodig blijkt. De aanleiding hiervoor kan bijvoorbeeld een risicovolle situatie zijn die nog niet in beeld was bij het opstellen van het jaarplan, of een bestuurlijke wens voor nader onderzoek, bijvoorbeeld omdat de gemeenteraad hierom vraagt. In die gevallen wordt, voordat een audit begint, dit vooraf gemeld aan de gemeentesecretaris en de VIC.

De AVG is omvangrijk. Audits zullen daarom onderwerp gewijs worden uitgevoerd. De volgende stappen worden daarbij doorlopen:

a. Voor aanvang van een onderzoek wordt alle relevante informatie verzameld;
b. Het bepalen van de sleutelfiguren die van belang zijn voor het onderzoek. Indien gewenst vindt vooraf een interview plaats om aandachtsgebieden te bepalen en actualiteiten mee te nemen;
c. Bepalen van de omvang van het onderzoek en het vaststellen van criteria van wat goed of niet goed is;
d. De uitvoering van het onderzoek;
e. De resultaten beoordelen en verifiëren;
f. De resultaten terugleggen aan verantwoordelijken voor hoor en wederhoor;
g. Vastleggen afspraken over verbetertraject en wie waarvoor verantwoordelijk is;
h. Het documenteren van de onderzoeksgegevens;
i. Rapporteren;
j. Monitoring.

4.4. KWALITEIT VAN DOOR DE FG UITGEVOERDE ONDERZOEKEN

Om de kwaliteit van een door de FG uitgevoerd onderzoek te kunnen borgen is het noodzakelijk dat een audit voldoet aan bepaalde kwaliteitscriteria.

De kwaliteitscriteria die de FG hanteert bij het doen van onderzoek zijn:

- onafhankelijkheid;
- risicogedreven benadering;
- toetsbaarheid;
- transparantie in onderzoek en rapportage;
- betrouwbaarheid;
- validiteit;
- informativiteit.

De AVG en het Statuut Functionaris Gegevensbescherming[9] voorzien de FG van bevoegdheden en middelen om onderzoeken conform genoemde kwaliteitscriteria uit te kunnen voeren. De volgende bepalingen uit het Statuut zijn in het kader van dit plan met name van belang:

- De FG ontvangt geen instructies met betrekking tot de uitvoering van zijn taken.
- De organisatie ondersteunt de FG bij de vervulling van zijn taken door hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid.

- De FG heeft de bevoegdheid om ongevraagd alle gemeentelijke ruimtes te betreden indien dit noodzakelijk is voor de uitoefening van zijn taak.

- De FG heeft in relatie tot zijn taken de bevoegdheid om inlichtingen en inzage te vragen en om zaken te onderzoeken.

- De FG wordt naar behoren en tijdig betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

5. RAPPORTAGES

5.1. INLEIDING

Om de voortgang te kunnen monitoren, zo nodig tijdig bij te kunnen sturen en om invulling te kunnen geven aan de verantwoordingsplicht dienen bestuur, management en de toezichthouder (FG) periodiek geïnformeerd te worden over de naleving van privacywet- en regelgeving en -beleid. In het vastgestelde privacy beleidskader zijn de verantwoordelijk-
heden in dit verband vastgelegd[10]. De rapportagevorm en de rapportagemomenten zijn in dit hoofdstuk nader uitgewerkt.

5.2. RAPPORTAGES DIE GERICHT ZIJN AAN DE GEMEENTERAAD

Volgens het privacy beleidskader[11] leggen het college en de burgemeester verantwoording af aan de raad over de status van de uitvoering van het privacy beleid en zullen zij *binnen de jaarlijkse planning & control cyclus* de gemeenteraad informeren over de risico's en over de getroffen beheersmaatregelen op het gebied van privacy. Conform het beleidskader zal deze rapportage binnen de paragraaf bedrijfsvoering van de jaarrekening plaatsvinden. De rapportage zal zich concentreren op hoofdlijnen. Hiertoe kan een samenvatting van de jaarrapportage van de FG[12] worden opgenomen in de paragraaf bedrijfsvoering.

---

[9] De uit het Statuut voortvloeiende taken en bevoegdheden van de FG zijn geïncorporeerd in het Organisatiebesluit

[10] Zie hoofdstuk 2 Privacy beleidskader gemeente Venlo

[11] Paragraaf 2.2

[12] Het betreft hier de jaarrapportage van de FG aan college en burgemeester gezamenlijk, waarvoor de FG het model zoals opgenomen in bijlage 4 gebruikt

Als de raad vragen heeft over de naleving van het privacy beleidskader bij de uitoefening van een specifieke gemeentelijke taak, kunnen deze vragen gesteld worden.

Verder vermeldt het privacy beleidskader dat het college en de burgemeester bijzonderheden ten aanzien van gegevensverwerkingen proactief aan de gemeenteraad melden, waarbij het voorbeeld wordt gegeven van ernstige datalekken. Dat zal gebeuren door middel van een raadsinformatiebrief.

Voor zover de gemeenteraad verantwoordelijk is voor verwerkingen van persoonsgegevens rapporteert de FG rechtstreeks aan de gemeenteraad. De FG zal het model jaarrapportage gegevensbescherming van de Informatiebeveiligingsdienst (IBD) (bijlage 3) gebruiken voor het maken van rapportages over de naleving van privacywetgeving en beleid ten aanzien van verwerkingen waarvoor de gemeenteraad verantwoordelijk is. Het model voorziet in een rapportage over de stand van zaken op ieder van de zeven thema's van het borgingsproduct[13].

Anders dan in het model jaarrapportage van de IBD, zal de rapportage van de FG richting de gemeenteraad geen managementsamenvatting uit de rapportage van de FG aan het college en de burgemeester bevatten. Het college legt (conform het vastgestelde privacy beleidskader) zelf verantwoording af over het gevoerde beleid via de reguliere planning en control cyclus, zodat de raad zijn taken als controlerend orgaan kan vervullen.

5.3. RAPPORTAGES DIE GERICHT ZIJN AAN COLLEGE, BURGEMEESTER, MANAGEMENT EN FG

In het privacy beleidskader staat beschreven op welke wijze vanuit de eerste, tweede en derde lijn verantwoording afgelegd wordt over de naleving van privacywetgeving en -beleid. Via werkoverleggen en binnen de HR gesprekcyclus brengen werknemers verslag uit aan hoofden. Hoofden rapporteren via verantwoordingsgesprekken richting de directie. Onderdeel van het daarvoor gebruikte format zijn privacy en dataprotectie.

Ook de FG rapporteert periodiek richting het management en aan het bestuur. Hierbij maakt hij gebruik van het model jaarrapportage gegevensbescherming van de Informatiebeveiligingsdienst (IBD), dat ziet op verwerkingen waarvoor het college en de burgemeester verantwoordelijk zijn (zie bijlage 4). In dit plan wordt er voor gekozen om de rapportage richting college en burgemeester in één jaarrapportage te bundelen. Naast de jaarrapportage rapporteert de FG over uitgevoerde audits.

In onderstaand overzicht staan de verschillende rapportagemomenten weergegeven. Voor de volledigheid is de VIC rapportage hieraan toegevoegd (zie hoofdstuk 2).

[13] Zie paragraaf 3.2

Tabel 1 - Rapportages

Rapport	Wanneer	In opdracht van	Door	Aan
Jaarrapportage FG	Jaarrekening	Raad, B&W en Burgemeester	FG	Raad/B&W/Burgemeester/Directie
Audits	Conform jaarplanning	Raad, B&W of Burgemeester	FG	Raad/B&W/Burgemeester/Directie
VIC rapportage	Jaarlijks	Directie	VIC	Directie, Concerncontroller, Business controllers, FG

Bijlage 1: AVG Borgingsproduct versie 2.0

https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2021/03/AVG-Borgingsproduct-2.0-definitief-1.xlsx

Bijlage 2: Handreiking AVG borgingsproduct 2.0

https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2021/03/Handreiking-AVG-borgingsproduct-2-definitief-1.docx

Bijlage 3: FG Jaarrapportage model gemeenteraad

2019-FG-Jaarrapportage-voorbeeld-Gem

Bijlage 4: FG Jaarrapportage model college en burgemeester

2019-FG-Jaarrapportage-voorbeeld-Coll


venlo