JAARVERSLAG FUNCTIONARIS GEGEVENSBESCHERMING GEMEENTE BEEMSTER 2018

Gemeenteraad

Over AVG-golven

Christel de Haan

4 maart 2019

VOORWOORD

Sinds 8 mei 2018 ben ik de Functionaris Gegevensbescherming van de (verwerkingsverantwoordelijken van de) gemeente Beemster.

Anders dan sommige collega's in den lande wil ik niet alleen een toezichthouder zijn. Ik wil ook een – tweedelijns - adviseur zijn van iedereen die, net als ik, vindt dat gegevensbescherming onderdeel moet uitmaken van het DNA van deze organisatie en van haar medewerkers, maar óók van iedereen die dat (nog) niet vindt. Tenslotte hoop ik een vertrouwde vraagbaak te worden van diegenen wiens persoonsgegevens binnen de gemeente verwerkt worden.

De gemeente Beemster is nog niet AVG-proof. Daarin bevinden we ons in goed gezelschap van heel veel andere (gemeentelijke) organisaties. Belangrijker is echter de constatering dat de aandacht voor gegevensbescherming binnen de organisatie het afgelopen jaar sterk gegroeid is.

In mijn eerste jaarverslag een terugblik op het "roerige" privacyjaar 2018 en een vooruitblik naar 2019.
Ik hoop u als lezer van dit verslag het komende jaar weer tegen te komen en samen met u de schouders te zetten onder dit belangrijke onderwerp.

Beemster, 4 maart 2019
Christel de Haan

INHOUDSOPGAVE

Samenvatting

Op 25 mei 2018 is de Algemene verordening gegevensbescherming in werking getreden. Voorafgaand aan deze datum hebben de verwerkingsverantwoordelijken van de gemeente Beemster de nodige besluiten genomen en processen ingericht. Deze maatregelen hielpen om na 25 mei in te kunnen spelen op vragen van buiten én vanuit de organisatie.
Het voorgaande wil niet zeggen dat de verwerkingsverantwoordelijken c.q. de Beemster gemeentelijke organisatie AVG-proof zijn (voor zover dit überhaupt óóit het geval zal zijn):
- van de in het privacybeleid opgenomen acties is een deel opgepakt en voltooid; een deel opgepakt, maar nog niet voltooid en een deel nog niet opgepakt;
- burgers en medewerkers geven signalen aan de Functionaris Gegevensbescherming af m.b.t. zaken waar zij zich vanuit privacy-oogpunt zorgen om maken;
- tenslotte constateer ik als Functionaris Gegevensbescherming ook zelf een aantal privacy-knelpunten binnen de organisatie.

De bescherming van de persoonsgegevens van de betrokkenen hoort een permanent aandachtspunt van verwerkingsverantwoordelijken, management en medewerkers te zijn. Door de komst van de nieuwe ondersteuner is de verwachting dat de rollen en taken van zowel de Functionaris Gegevensbescherming als de privacyfunctionaris beter tot hun recht zullen komen. Bedoeling is de privacy-volwassenheid van de gemeentelijke organisatie hiermee naar een hoger plan te tillen.

Verklarende woordenlijst

- Algemene verordening gegevensbescherming (AVG):
  Europese verordening die regels stelt over privacy.
- Autoriteit Persoonsgegevens (AP):
  de organisatie die in Nederland toezicht houdt op de naleving van de AVG.
- Betrokkene:
  degene wiens persoonsgegevens door een verwerkingsverantwoordelijke van de gemeente verwerkt worden.
- Chief Information Security Officer (CISO):
  adviseur en deskundige op het vlak van het identificeren, voorkomen en verminderen van (technische) IT-beveiligingsrisico's.
- Functionaris Gegevensbescherming (FG):
  onafhankelijke adviseur van en toezichthouder op (de naleving van de privacywetgeving door) de verwerkingsverantwoordelijken. Tevens aanspreekpunt en contactpersoon voor betrokkenen en AP inzake privacy-aangelegenheden.
- Gegevensbeschermingseffectbeoordeling (DPIA):
  analyse van een (voorgenomen) gegevensverwerking die waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen.
- Gegevenseigenaar:
  degene die materieel verantwoordelijk is voor de persoonsgegevens die binnen zijn taakgebied worden verwerkt. Binnen Purmerend (als verwerker van de Beemster gegevensverwerkingen) worden dat – naar verwachting – de teammanagers en de projectleiders.
- Privacy:
  informationele privacy ofwel bescherming van persoonsgegevens.
- Verwerker:
  degene die als dienst voor een verwerkingsverantwoordelijke persoonsgegevens verwerkt. Voorbeeld: de gemeente Purmerend en de leveranciers van systemen als Suite en Youforce.

- Verwerkingsverantwoordelijke:
  degene die formeel verantwoordelijk is voor de persoonsgegevens die binnen zijn taakgebied worden verwerkt. Binnen de gemeente zijn dat: het college van burgemeester en wethouders, de gemeenteraad, de burgemeester, de heffingsambtenaar, de ambtenaar burgerlijke stand, de leerplichtambtenaar en de toezichthouder Wmo.

Deel 1 Terugblik op 2018, de eerste AVG-golf

1.1 De weg naar 25 mei 2018

25 mei 2018, de dag waarop de AVG van toepassing werd op alle verwerkingen van persoonsgegevens binnen de Europese Unie. Voorafgaand aan die dag bereikte de eerste AVG-golf de Nederlandse kust. Dit was een golf van hectiek, soms zelfs van paniek en zij voerde allerlei producten mee die in allerijl in organisaties werden geïmplementeerd om “op het oog” AVG-proof te zijn.

De eerste AVG-golf stroomde ook door de Beemster organisatie. In haar kielzog zijn door de verwerkingsverantwoordelijken de volgende acties ondernomen c.q. besluiten genomen:
- aanwijzing van de FG;
- vaststelling van het privacybeleid, door het college en de burgemeester;
- (start van de) inrichting van het register van verwerkingsactiviteiten;
- inrichten van het register datalekken;
- (start van de) vastlegging van de procedures inzake vormgeving rechten van betrokkenen.

Was alle hectiek c.q. waren alle genomen maatregelen vóór 25 mei 2018 terecht? Ja.
Sinds 25 mei 2018 is gebleken dat er permanent aandacht gevraagd wordt voor privacy:
- vanuit de burger (middels het inroepen van zijn rechten);
- vanuit de AP (middels het doen van onderzoeken naar AVG-conformiteit); en
- vanuit de pers (middels het herhaaldelijk publiceren over datalekken en recentelijk nog over de zorgen die burgers zich maken over privacy).

De voorbereidende werkzaamheden c.q. genomen besluiten bieden (deels) de onderligger voor de reactie hierop.

1.2 Doelen en acties uit het privacybeleid en hun stand van zaken (1)

In het privacybeleid staan onderstaande privacy-acties benoemd.[1]
[2]

1.	**Vaststellen privacybeleid** Het beleid is door de gemeenteraad vastgesteld op 29 mei 2018 en na publicatie in het gemeenteblad op 6 juni 2018 in werking getreden	
2.	**Aanwijzen FG** De FG is op 8 mei 2018 aangewezen door alle Beemster verwerkingsverantwoordelijken	
3.	Opstellen register van verwerkingsactiviteiten	
4.	**Opstellen en bijhouden register datalekken** Sinds 1 mei 2018 worden in het register alle (gemelde) datalekken bijgehouden	
5.	Beschikbaar hebben DPIA’s	
6.	Uitvoeren DPIA’s	
7.	Daar waar toestemming de grondslag voor gegevensverwerking is, kunnen aantonen dat toestemming is gegeven	
8.	Beoordelen rechtmatigheid gegevensverwerkingen	
9.	**Vormgeven proces rechten betrokkenen** Op internet én op het Purmerendse intranet staan model-brieven en model-besluiten	

[1] *NB De acties uit het privacybeleid die te maken hebben met informatiebeveiliging, worden inhoudelijk besproken in het jaarverslag van de CISO en zijn hier daarom niet verder genoemd*.
[2] Verklaring kleuren in tabel: groen = afgeronde actie; oranje = actie opgepakt, nog niet afgerond; rood = actie nog niet opgepakt

10.	Afsluiten verwerkersovereenkomsten	
11.	Stimuleren privacycultuur/voeren privacybewustwordingscampagnes	
12.	**Inrichten Purmerendse intranetpagina Privacy & Informatiebeveiliging** De “PIB-space” is ingericht en wordt regelmatig geüpdatet. In de loop van 2019 ondergaat de look van de pagina een professionaliseringsslag	
	Inrichten internetpagina Privacy Ook deze pagina wordt geactualiseerd wanneer dat nodig is en wordt door IB&P bestempeld als inspiratiebron voor andere gemeenten	
13.	**Opzetten privacy-werkgroepen** Inmiddels vinden in Purmerend regelmatig vergaderingen plaats van de gemeentebrede werkgroep en van de sub-werkgroepen Maatschappelijk Domein/archief/ VBA	
14.	Implementeren organisatorische privacy by design	
15.	Opstellen procesbeschrijvingen	

De afgeronde acties worden nu niet verder besproken. Uiteraard zullen de verwerkingsverantwoordelijken[3] ervoor moeten zorgen dat deze acties op groen blíjven staan.

1.3 Doelen en acties uit het privacybeleid en hun stand van zaken (2)

Aandacht verdienen de oranje en rode actiepunten.

Oranje actiepunten; zaken die zijn opgepakt, maar nog niet zijn afgerond.

1. Opstellen register van verwerkingsactiviteiten
   Op 1 februari 2018 is gestart met het opstellen van dit register. Op het moment van schrijven van dit verslag wordt hier nog steeds aan gewerkt. Inmiddels zijn zo’n 25 verwerkingen waarvoor de gemeenteraad verwerkingsverantwoordelijke is, in beeld. Denk hierbij aan P&O verwerkingen t.b.v. griffiepersoneel, maar ook aan verwerkingen in verband met ingediende bezwaarschriften en zienswijzen bestemmingsplannen.
   De AVG bepaalt niet het detailniveau van het register. De AP eist wel een dusdanig niveau dat zowel voor betrokkenen als voor de organisatie zelf helder is hoe met een individuele verwerking wordt omgegaan.
   Het register van verwerkingsactiviteiten is in het kader van de transparantie zowel door de verwerkingsverantwoordelijken van Purmerend als van Beemster gepubliceerd op internet. In een uitgebreidere versie is het register ook op intranet te vinden.
2. Toestemming als grondslag en de aantoonbaarheid daarvan
   Toestemming is één van de 6 grondslagen om persoonsgegevens te mogen verwerken. Om rechtmatig van deze grondslag gebruik te kunnen maken moet toestemming vrij/specifiek/geïnformeerd en ondubbelzinnig gegeven zijn. Een eenmaal gegeven toestemming kan t.a.t. worden ingetrokken. Een eenmaal gegeven toestemming kan t.a.t. worden ingetrokken en is sowieso beperkt geldig (afhankelijk van het onderwerp maximaal 1-3 jaar). Deze eisen maken “toestemming” tot een zoveel mogelijk te vermijden grondslag. Desalniettemin is en wordt (veel) gebruik gemaakt van deze grondslag.
   Het onderzoek waar deze grondslag rechtmatig kan worden toegepast en het aanpassen van formulieren om deze toestemming ook aantoonbaar te maken, vindt incidenteel plaats.

[3] Feitelijk: de hieronder genoemde gegevenseigenaren

In 2019 zal door de FG meer aandacht aan de grondslag toestemming besteed worden.

3. Beoordelen rechtmatigheid gegevensverwerkingen
   Het register van verwerkingsactiviteiten bevat het overzicht van de gegevens-verwerkingen binnen de organisatie. Bij het vullen van het register wordt een eerste screening gedaan van de rechtmatigheid van de verwerking. Na voltooiing van het register zullen – met name de hoog risico-verwerkingen verder op rechtmatigheid getoetst worden. Dergelijke hoog risico-verwerkingen vinden vooral plaats onder verantwoordelijkheid van het college en de burgemeester.
4. Afsluiten verwerkersovereenkomsten
   Een verwerkingsverantwoordelijke mag een externe verwerker inschakelen om namens hem persoonsgegevens te verwerken. De gemeente Purmerend als verwerker is hier het meest duidelijke voorbeeld van. Verwerkers mogen alleen worden ingeschakeld als goede afspraken zijn gemaakt over de wijze van verwerking en de mate van beveiliging ervan. Met diverse verwerkers blijken die afspraken echter nog niet te zijn gemaakt. Dit actiepunt wordt door de FG samen met de privacyfunctionaris opgepakt.
5. Stimuleren privacycultuur/voeren privacybewustwordingscampagnes
   Dit is een permanent punt van aandacht dat een vast onderdeel zou moeten zijn in besprekingen van managers met hun medewerkers.
6. Implementeren organisatorische privacy by design
   Privacy by design in systemen is door een verwerkingsverantwoordelijke niet altijd te beïnvloeden. Het implementeren van organisatorische privacy by design heeft hij echter zelf in de hand.
7. Opstellen procesbeschrijvingen
   Inmiddels is de procesbeschrijving inzageverzoek persoonsgegevens vastgesteld. Nagegaan moet worden welke andere privacy-processen zich voor een procesbeschrijving lenen.

Rode actiepunten; zaken die nog niet zijn opgepakt.
DPIA's. Binnen de informatiebeveiliging worden regelmatig (verkorte) risicoanalyses uitgevoerd om na te gaan welke risico's kleven aan een nieuwe systeem c.q. aan een nieuwe applicatie en welke maatregelen nodig zijn om deze risico's te ondervangen. Analyses, puur vanuit privacy-perspectief, worden voor Beemster nog niet opgepakt.
De AP heeft inmiddels een lijst uitgebracht met verwerkingen waarvoor in ieder geval een DPIA moet worden uitgevoerd. Deze lijst is recent uitgebreid met DPIA-checklists voor bestaande resp. nieuwe verwerkingen. De VNG zal op korte termijn een AVG-tool ter beschikking stellen.
Aan de hand van deze lijst, checklists en tool moet worden nagegaan voor welke gegevensverwerkingen een DPIA (alsnog) uitgevoerd moet worden. In eerste instantie zullen dat vooral verwerkingen zijn waarvoor het college en de burgemeester verwerkingsverantwoordelijke zijn, denk aan verwerkingen in samenwerkingsverbanden zoals het Veiligheidshuis. Op basis van de nu voorliggende lijst van de AP zullen gegevensverwerkingen van de raad niet snel aan een DPIA onderworpen moeten worden.

1.4 Het meldpunt datalekken

Sinds 1 januari 2016 bemannen de CISO en de FG het meldpunt datalekken. Inmiddels maken ook de privacyfunctionaris en de plv. CISO deel uit van het meldpunt.
Samen hebben zij in 2018 diverse datalekken behandeld waarvan er geen onder de verantwoordelijkheid van de Beemster gemeenteraad viel.

Sinds 25 mei 2018 hanteert de AP andere criteria voor het melden van datalekken. Niet langer meldingswaardig zijn datalekken waarbij de onbevoegde ontvanger als "betrouwbaar" kan worden beschouwd. "Betrouwbaar" kwalificeert de AP de volgende groepen personen:

- personen waarmee de verwerkingsverantwoordelijke een langere zakelijke relatie onderhoudt;
- personen met een (tuchtrechtelijk afdwingbaar) beroepsgeheim, zoals een huisarts;
- personen met een geheimhoudingsplicht, zoals een ambtenaar.

Met name die laatste kwalificatie heeft tot gevolg dat interne datalekken zoals het bovengenoemde, niet meer gemeld worden aan de AP.

De AVG eist dat verwerkingsverantwoordelijken een register datalekken hebben. Voor Purmerend en Beemster wordt dit register sinds 1 mei 2018 bijgehouden door het meldpunt datalekken. Dit register is niet openbaar en is uitsluitend toegankelijk voor de betreffende verwerkingsverantwoordelijke, het meldpunt en de AP.

De CISO heeft in zijn jaarverslag Informatiebeveiliging 2018 aandacht besteed aan de behandeling van datalekken. Hier wordt verder volstaan met een verwijzing naar dit stuk.

1.5 Signalen en interventies

Betrokkenen kunnen o.g.v. de AVG met de FG contact opnemen over “alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten”. Bovendien wil ik als FG voor medewerkers én burgers een laagdrempelig aanspreekpunt zijn voor alle zaken waarover zij zich vanuit privacy-oogpunt zorgen maken (en die te maken hebben met de gemeentelijke organisatie).

Het bovenstaande leidde in 2018 tot signalen en interventies:

1. **Burgers**
   - 2 interventie t.a.v. processen waarvoor het college van Purmerend de verwerkingsverantwoordelijke was
   - 1 bemiddeling t.a.v. een proces waarvoor de burgemeester van Purmerend de verwerkingsverantwoordelijke was
2. **Medewerkers**
   20 signalen t.a.v. processen waarvoor het college resp. de burgemeester van Purmerend en Beemster de verwerkingsverantwoordelijken waren.

1.6 (aanvullende) Knelpunten

Naast de signalen van burgers en medewerkers en de nog niet afgeronde actiepunten uit het privacybeleid, signaleer ik– in ieder geval – de volgende knelpunten, voor zover ze ook voor de gemeenteraad als verwerkingsverantwoordelijke relevant zijn:

- <u>Bewaartermijnen</u>
  Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk[4] voor het doel waarvoor ze verzameld zijn. (Kopieën) van eenmaal verzamelde gegevens blijven echter vaak veel langer bewaard dan noodzakelijk in o.a. mailboxen en L- of M-schijven, terwijl ze óf vernietigd óf gearchiveerd moeten worden.
- <u>Logging</u>
  Medewerkers mogen dié persoonsgegevens verwerken die noodzakelijk zijn bij de uitvoering van hun taken; zij horen geen toegang te hebben tot andere persoonsgegevens. Eén van de manieren om te controleren of ook inderdaad geen toegang is geweest tot andere persoonsgegevens is logging. Logging is nog niet standaard ingebouwd in de (grote) gemeentelijke systemen. De AP controleert actief op het hebben én controleren van loggegevens.
- <u>Register verwerkingsactiviteiten vanuit verwerkersrol</u>
  De AVG eist van een organisatie een overzicht van de verwerkingen die zij uitvoert

[4] De termijn waarbinnen gegevens bewaard mogen blijven is niet in absolute termen uit te drukken. Gegevens van een griffiemedewerker die 25 jaar in dienst is kunnen 25 jaar noodzakelijk zijn en dus rechtmatig bewaard worden. De gegevens in een onterecht bij de raad binnengekomen mail moeten per omgaande verwijderd worden.

vanuit de rol van verwerkingsverantwoordelijke; hierboven werd daarop al ingegaan. De AVG eist van een organisatie echter ook een overzicht van verwerkingen die zij uitvoert vanuit de rol van verwerker. Voor Beemster is een dergelijk overzicht er niet; nagegaan moet worden of Beemster nog voor een organisatie de verwerkersrol vervult.

- Verhouding (bewaartermijnen) AVG en Archiefwet
  Dit punt heeft inmiddels landelijke aandacht, maar kan ook als gemeentelijk knelpunt genoemd worden.
  Zowel de AVG als de Archiefwet kennen bewaartermijnen. Als Europese wet gaat de AVG vóór de Archiefwet. Vragen die uit de verhouding tussen beide wetten voortkomen zijn:
  - Hoe moet gewerkt worden met systemen die zijn ingeregeld op Archiefwet-bewaartermijnen en niet op AVG-bewaartermijnen?
  - Vallen alle stukken die op het stadhuis van Purmerend t.b.v. Beemster geproduceerd worden onder de Archiefwet of is op deze stukken uitsluitend de AVG van toepassing? Hierbij moet bijvoorbeeld gedacht worden aan de gegevens die P&O heeft van de (griffie)medewerkers.

  Het is van belang de landelijke ontwikkelingen op dit onderwerp te blijven volgen.
- Gegevenseigenaren
  Taken op het gebied van privacy worden nu veelal geïnitieerd, gecoördineerd en uitgevoerd door de privacyfunctionaris en de FG. Veel van die taken horen echter bij de gegevenseigenaren thuis; denk aan het doorgeven van wijzigingen in de registers van verwerkingsactiviteiten en het actueel houden van verwerkersovereenkomsten. De regisseur gegevensbeheer is momenteel bezig de rol van gegevenseigenaar verder in te vullen.
- (toekomstig) Zaaksysteem
  Een zaaksysteem is een belangrijk instrument bij een goede interne informatievoorziening. Een zaaksysteem echter waarmee een medewerker met één druk op de knop én zonder een noodzaak daartoe, de toegang krijgt tot een deel van de Brp-gegevens van álle Nederlanders, is een permanente bron van datalekken.
- Uitwisseling persoonsgegevens met ketenpartners
  Uit de aard van de gemeentelijke taken vloeien veelvuldige uitwisselingen van persoonsgegevens met ketenpartners voort. Voor zover uitwisselingen al in beeld zijn, vinden ze niet altijd overeenkomst de privacywetgeving plaats en verdienen daarom verdere aandacht op privacygebied.

1.7 “Team FG”; taken en werkdruk FG en privacyfunctionaris + komst ondersteuner

De FG heeft op grond van de AVG de volgende taken:
- De verwerkingsverantwoordelijke/de verwerker informeren en adviseren over zijn verplichtingen o.g.v. de privacywetgeving;
- Toezien op de naleving van privacywetgeving en beleid;
- Adviseren over en toezien op de uitvoering van DPIA’s;
- Samenwerken met en optreden als contactpunt van de AP;
- Aanspreekpunt voor betrokkenen over alle zaken die verband houden met de verwerking van hun persoonsgegevens en met de uitoefening van hun rechten o.g.v. de AVG.

Via het privacybeleid zijn daar de volgende taken aan toegevoegd:
- Voorzitterschap van de privacy-werkgroepen;
- Bijhouden van het register van verwerkingsactiviteiten (nadat de wijzigingen door de gegevenseigenaar zijn doorgegeven);
- Onderdeel van het meldpunt datalekken;
- Sparringpartner van de CISO.

Ik ben op 8 mei 2018 aangewezen als FG van de verwerkingsverantwoordelijken van de gemeente Beemster. Sindsdien zijn daar ook het FG-schap van (de verwerkingsverantwoordelijken van) het Waterlands Archief en Werkom bij gekomen.

De privacyfunctionaris heeft o.g.v. het gemeentelijke privacybeleid de volgende taken:

- Dagdagelijks aanspreekpunt voor vragen over privacy;
- Ondersteunen bij het opstellen van verwerkersovereenkomsten;
- Opstellen van privacy-modellen;
- Lid van de privacy-werkgroepen;
- Bijhouden van het register van verwerkingsactiviteiten (nadat de wijzigingen door de gegevenseigenaar aan de privacyfunctionaris resp. FG zijn doorgegeven);
- Onderdeel van het meldpunt datalekken;
- Vervangen van de FG bij diens afwezigheid.

Sinds 1 november 2018 heeft Purmerend, óók voor Beemster, een vaste privacyfunctionaris voor 16 uur per week.

In 2018 hebben de privacyfunctionaris en de FG een stroom aan vragen beantwoord over de implementatie en uitleg van de AVG. De omvang van die stroom, in combinatie met de werkzaamheden die de FG ook voor andere organisaties verricht, leidt tot het op 13 februari 2019 benoemen van een tijdelijke ondersteuner.
De verwachting is dat de FG en de privacyfunctionaris met de komst van de ondersteuner in staat zullen zijn hun rollen zuiverder op te pakken. De FG zal vanaf nu vooral tweedelijns adviseur zijn van medewerkers. Eerstelijns adviseur is de FG dan van de verwerkingsverantwoordelijken van Beemster, de gemeente Purmerend als verwerker van de verwerkingsverantwoordelijken van Beemster, de gegevenseigenaren, de privacyambassadeurs in de werkgroepen, de privacyfunctionaris en bij principiële privacy-aangelegenheden in een team.

Deel 2 Vooruitblik op 2019, de tweede AVG-golf

2.1 Op weg naar borging

Waar de eerste Nederlandse AVG-golf zich kenmerkte door hectiek en deels door "window-dressing", kenmerkt de tweede AVG-golf zich door het besef dat privacy geen onderwerp is dat "wel weer overwaait" en daarom structurele borging vereist in de organisatie. Ter ondersteuning hiervan hebben VNG en IBD (InformatieBeveiligingsDienst) in december 2018 een document uit met de titel: Het borgen van de AVG in de gemeentelijke organisatie uitgebracht.

Borging wordt in het Beemster privacybeleid als volgt verwoord:
Volledig voldoen aan de eisen die de privacywetten aan de gemeentelijke organisatie stellen, betekent voldoen aan c.q. in het bezit zijn van alle in bovengenoemde elementen opgenomen punten/stukken + het actueel houden hiervan via een plan-do-check-act cyclus.

Het is aan de gemeentelijke organisatie om die borging vorm te geven c.q. om die PDCA-cyclus te doorlopen. Het is aan de FG om erop toe te zien dat deze borging ook daadwerkelijk gestalte krijgt. Het is óók aan de FG om daar waar nodig te adviseren over de vormgeving van die borging.

Hieronder een overzicht van de plannen van de FG voor 2019 op weg naar gemeentelijke borging van de AVG. Hierbij wordt een onderscheid gemaakt tussen structurele actiepunten en incidentele/thematische actiepunten[5].

2.1.1 Acties uit 2018 die in 2019 een vervolg krijgen

Structurele actiepunten

	Actiepunt	Toelichting	Planning
1.	bijhouden register van verwerkingsactiviteiten	het register is de basis voor inzicht in gegevensverwerkingen; actueel houden is prioriteit 1	vanaf K2[6]
2.	beoordelen rechtmatigheid gegevensverwerkingen	begonnen wordt met beoordeling van de hoog risico-verwerkingen die onder de verantwoordelijkheid van burgemeester en wethouders resp. de burgemeester vallen	vanaf K2
3.	monitoren aanwezigheid verwerkersovereen-komsten	óók voor het geval de gemeente Beemster verwerker is	vanaf K1
4.	vergroten en onderhouden privacycultuur	de FG speelt hier een actieve rol in, o.a. via het geven van presentaties en het voorzitterschap van de privacy-werkgroepen	vanaf K1
5.	monitoren vormgeven organisatorische privacy by design	met actiepunt 6 vormt dit punt de basis voor medewerkers om privacyproof te kúnnen werken	vanaf K1
6.	monitoren vormgeven privacy by design in systemen	dit punt wordt in samenwerking met de CISO (en waar mogelijk/nodig met externe organisaties) opgepakt	vanaf K2
7.	uitvoeren DPIA's	de FG speelt hier een actieve rol in	Vanaf K2

[5] NB incidentele actiepunten die onvoldoende resultaat opleveren, worden vervolgd in een volgend jaar of toegevoegd aan de structurele actiepunten
[6] K= Kwartaal

		a.h.v. de DPIA-lijst van de AP; verwerkingen waarvoor de gemeenteraad verwerkings-verantwoordelijke is, zullen niet snel aan een DPIA onderworpen worden	
8.	up to date houden internet pagina privacy en PIB space op intranet	de FG speelt hier een actieve rol in	vanaf K1

Incidentele/thematische actiepunten

	Actiepunt	**Toelichting**	**Planning**
1.	opstellen register van verwerkingsactiviteiten		K1, K2
2.	Beoordelen rechtmatig toepassen grondslag toestemming	opgepakt in combinatie met structureel actiepunt 2	K2-4
3.	opstellen proces-beschrijvingen privacy-processen (rechten betrokkenen)	spitst zich in eerste instantie toe op een inventarisatie van de behoefte naar nieuwe procesbeschrijvingen; actiepunt wordt uitgezet in de privacy-werkgroepen, waardoor hier ook een actieve rol voor de FG is weggelegd	K2 (met ev. vervolg)
4.	beschikbaar hebben standaard-DPIA	als mogelijk aansluiten bij in ontwikkeling zijnde DPIA tool van de VNG; dit punt wordt in samenwerking met de CISO opgepakt (zie opmerking bij structureel actiepunt 7)	K2, K3

2.1.2 Nieuwe acties voor 2019

Structurele actiepunten

	Actiepunt	**Toelichting**	**Planning**
1.	Gesprek aangaan met de griffier en waar nodig het raadspresidium over de in bijlage 1 opgenomen AVG-borgingstabel	- Deels overlapt dit punt de actiepunten genoemd onder 2.1.1 - vindt plaats met inachtneming van de uitkomsten van incidenteel actiepunt 2 (2019) - de resultaten hiervan vormen de basis voor een eerste GAP-analyse	Vanaf K2

Incidentele/thematische actiepunten

	Actiepunt	**Toelichting**	**Planning**
1.	Besluitvorming voorbereiden over ev. aanschaf PMS/ISMS[7]		K2
2.	Gesprek aangaan met het raadspresidium over (gewenst) niveau van	Gesprekken met de griffier (structureel actiepunt 1 (2019)) hebben zin wanneer bekend is wat	K2

[7] PMS = Privacy Management System; ISMS = Informatie Security Management System

	privacy volwassenheid	– voor nu - het gewenste eindniveau is	
3.	Met B&I en Communicatie verbeteren zichtbaarheid FG voor burgers en betrokkenen		K1, K2

Bijlage 1 Borging van de AVG in tabelvorm[8]

Privacybeleid

Activiteiten	onbekend/(nog) niet van toepassing	ontbreekt	onvoldoende/ niet gemeentebreed	voldoende	goed/afgerond
Is juridisch getoetst en goedgekeurd					X
Is vastgesteld door de verwerkingsverantwoordelijken					X
Is bekend gemaakt binnen en buiten de gemeente					X
Wordt door het management actief uitgedragen					
Is leidend bij ontwerp en ontwikkelen van (nieuwe) verwerkingen					
Is – waar nodig – domein specifiek uitgewerkt					
Er zijn afspraken/maatregelen over gegevensbescherming binnen de gemeente					
Wordt periodiek getoetst					
Privacyverklaring is gepubliceerd op de website					X

De FG

Activiteiten	onbekend/(nog) niet van toepassing	ontbreekt	onvoldoende/niet gemeentebreed	voldoende	goed/afgerond
Verwerkingsverantwoordelijken hebben een FG aangewezen					X
De FG wordt tijdig betrokken bij zaken die verband houden met privacy					
De FG beschikt over de middelen die hij nodig heeft om zijn functie uit te oefenen					
Betrokkenen kunnen op eenvoudige wijze contact opnemen met de FG					X
De FG brengt – in ieder geval – jaarlijks verslag uit					X

[8] Onderwerpen uit de tabel zijn afkomstig uit het VNG/IBD document “Het borgen van de AVG in de gemeentelijke organisatie”. Alleen de afgeronde actiepunten zijn ingevuld; over de overige punten wordt het gesprek aangegaan.

over de omgang met persoonsgegevens binnen de organisatie					

Organisatorische inbedding van de AVG

Activiteiten	onbekend/(nog) niet van toepassing	ontbreekt	onvoldoende/niet gemeentebreed	voldoende	goed/afgerond
Er is een privacyfunctionaris die op casusniveau adviseert omtrent privacy					X
Er zijn gegevenseigenaren aangewezen die verantwoordelijk zijn voor de privacy binnen hun team					
Er zijn privacyambassadeurs binnen de teams aangewezen					

Processen

Activiteiten	onbekend/(nog) niet van toepassing	ontbreekt	onvoldoende/ niet gemeentebreed	voldoende	goed/afgerond
In werkprocessen wordt waar nodig aandacht besteed aan gegevensbescherming					
Er zijn processen en voorzieningen voor het faciliteren van de rechten van betrokkenen					
De OR wordt actief geïnformeerd over dan wel om instemming gevraagd m.b.t. privacyregelingen die een effect hebben op het personeel					X
In ieder geval tekenen extérnen een integriteits- en geheimhoudingsverklaring					
Inzichtelijk is welke besluiten genomen worden op basis van geautomatiseerde besluitvorming					
Processen/systemen/de organisatie wordt ingericht volgens het principe van privacy by design/privacy by default					
De verwerkingsverantwoordelijken bepalen of en zo ja, welke maatregelen genomen moeten worden					

n.a.v. het verslag van de FG					
Burgers worden op de hoogte gehouden van de naleving van de AVG binnen de gemeente					

Register van verwerkingsactiviteiten

Activiteiten	**onbekend/(nog) niet van toepassing**	**ontbreekt**	**onvoldoende/niet gemeentebreed**	**voldoende**	**goed/afgerond**
Er is een volledig en actueel register van verwerkingsactiviteiten waarvoor de gemeente verwerkingsverantwoordelijke is					
Er is een volledig en actueel register van verwerkingsactiviteiten waarvoor de gemeente verwerker is					
De registers van verwerkingsactiviteiten zijn – voor zover mogelijk – openbaar c.q. kunnen ter beschikking worden gesteld van de AP					X
De registers van verwerkingsactiviteiten worden beheerd					X
Gegevenseigenaren weten aan wie zij wijzigingen van bestaande verwerkingen moeten doorgeven en doen dat ook					

DPIA's

Activiteiten	**onbekend/(nog) niet van toepassing**	**ontbreekt**	**onvoldoende/niet gemeentebreed**	**voldoende**	**goed/afgerond**
Er is een compleet en actueel beeld van bestaande verwerkingen die een hoog privacyrisico opleveren en waarvoor een DPIA is/moet worden uitgevoerd					
Er is een standaardformat beschikbaar voor DPIA's					
Er is een proces voor het uitvoeren van DPIA's					
De verwerkingsverantwoordelijke motiveert besluitvorming die afwijkt van het advies van de FG t.a.v. een DPIA					

Resultaten van DPIA's zijn geregistreerd en vindbaar voor betrokken medewerkers					
Resultaten van DPIA's worden teruggekoppeld naar betrokken medewerkers					
Op basis van DPIA's uit te voeren maatregelen worden uitgevoerd					
DPIA's worden periodiek – minimaal elke 3 jaar - herhaald					

Noodzakelijke kennis bij medewerkers

Activiteiten	**onbekend/(nog) niet van toepassing**	**ontbreekt**	**onvoldoende/niet gemeentebreed**	**voldoende**	**goed/afgerond**
Medewerkers weten wie de privacyambassadeur binnen hun team is					
Medewerkers zijn op de hoogte van de wijze waarop de gemeente met persoonsgegevens omgaat, inclusief de vormgeving van rechten van betrokkenen en het juist gebruik van grondslagen voor verwerking					
Medewerkers weten aan wie zij datalekken moeten doorgeven					
Medewerkers weten hoe zij met wijzigingen in verwerkingen moeten omgaan + aan wie ze die moeten doorgeven					
Waar nodig volgen medewerkers trainingen ter bevordering van het privacybewustzijn					

Autorisaties en controle daarop

Activiteiten	**onbekend/(nog) niet van toepassing**	**ontbreekt**	**onvoldoende/niet gemeentebreed**	**voldoende**	**goed/afgerond**
Een medewerker heeft de autorisaties die bij zijn functie horen; zij vervallen bij uitdiensttreding					
Zo mogelijk wordt middels logging gecontroleerd of					

de autorisaties juist zijn toegepast					

Vormgeving rechten betrokkenen

Activiteiten	**onbekend/(nog) niet van toepassing**	**ontbreekt**	**onvoldoende/niet gemeentebreed**	**voldoende**	**goed/afgerond**
Betrokkenen worden op algemene wijze geïnformeerd over hun rechten via de gemeentelijke website					X
Betrokkenen worden actief geïnformeerd over hun rechten bij (eerste) contact met de gemeente					
Betrokkenen worden tijdig geïnformeerd over de wijze waarop hun gegevens worden verwerkt					
“Toestemming” als rechtmatige grondslag voor een gegevensverwerking is aantoonbaar					
Betrokkenen worden geïnformeerd over de mogelijkheden om een (rechtmatig gegeven) toestemming in te trekken					

Samenwerking

Activiteiten	**onbekend/(nog) niet van toepassing**	**ontbreekt**	**onvoldoende/niet gemeentebreed**	**voldoende**	**goed/afgerond**
Inzichtelijk is aan welke externe partij meermaals persoonsgegevens verstrekt worden c.q. van welke externe partij persoonsgegevens ontvangen worden					
Inzichtelijk is of een externe partij met wie meermaals persoonsgegevens worden uitgewisseld dit doet vanuit de rol van verwerker, gezamenlijk verwerkingsverantwoordelijke, zelfstandig verwerkingsverantwoordelijke					
Afhankelijk van de rol die een externe partij heeft m.b.t. de uitwisseling van persoonsgegevens, worden tijdig passende afspraken gemaakt; deze worden vastgelegd in een verwerkersovereenkomst					

dan wel privacyconvenant					
Een eenmalige gegevensuitwisseling met een externe partij is AVG-proof; afhankelijk van de aard van de uitwisseling worden schriftelijk afspraken vastgelegd					

Datalekken

Activiteiten	**onbekend/(nog) niet van toepassing**	**ontbreekt**	**onvoldoende/niet gemeentebreed**	**voldoende**	**goed/afgerond**
Er is een proces m.b.t. de afhandeling van datalekken					X
Er is inzicht in alle datalekken die onder verantwoordelijkheid van de gemeente plaatsvinden					
Er is een register datalekken dat wordt beheerd					X