JAARVERSLAG FUNCTIONARIS GEGEVENSBESCHERMING GEMEENTE BEEMSTER 2019

Gemeenteraad

Over borging, successen en (terechte?) zorgen

Christel de Jong

18 april 2020

VOORWOORD

2019, het eerste volle jaar voor de AVG waarin in Beemster op privacygebied genoeg gebeurd is om weer een jaarverslag mee te vullen.
Een jaarverslag dat als titel heeft meegekregen: Over borging, successen en (terechte?) zorgen.

Ik wil u als lezer meenemen langs deze onderwerpen en hoop hiermee een beeld te geven van hoe de gemeente Beemster er vanuit -mijn- privacyperspectief voor staat.

Ik ga graag in gesprek over de vraag of u de gemeente in dit verslag herkent. En nog belangrijker: ik ga graag in gesprek over de vraag hoe we successen kunnen vieren en zorgen -zoveel mogelijk- kunnen wegnemen.

Voor de goede orde: ik heb ook jaarverslagen geschreven die gericht zijn aan respectievelijk het college en de burgemeester van Purmerend, de gemeenteraad van Purmerend en het college/de burgemeester van Beemster.

Beemster, 18 april 2020
Christel de Jong

INHOUDSOPGAVE

Samenvatting

Het eerste volle AVG-jaar. Er zijn successen te vieren en er zijn zorgen.
Successen zijn er op het vlak van privacy by design en de kennis van de AVG bij (griffie-) medewerkers. Successen uit 2018 worden echter niet altijd vastgehouden, terwijl dit wel van belang is.
Niet alle zorgen uit 2018 (van medewerkers en van de FG) zijn weggenomen; dit is ook niet realistisch. Wél mag verwacht worden dat er aandacht voor deze zorgen blijft. Denk hierbij aan zorgen over de manier waarop privacyproof in de regelmaatruimtes gewerkt kan worden.
Burgers weten de FG in 2019 te vinden met klachten. Deze klachten worden door de FG gebruikt om het gesprek met gegevenseigenaren aan te gaan en processen meer AVG-proof te maken.
Er zijn in 2019 2 datalekken door het meldpunt datalekken afgehandeld die mede onder de verantwoordelijkheid van de raad vielen. Dit is een kleine stijging t.o.v. 2018. De FG ziet de oorzaak van deze stijging meer in een groter privacybewustzijn bij de organisatie en in een betere bekendheid van het meldpunt, dan in het onzorgvuldiger verwerken van persoonsgegevens.

Verklarende woordenlijst

- Autoriteit Persoonsgegevens (AP):
  de Nederlandse toezichthouder op de naleving van de AVG.
- Betrokkene:
  degene wiens persoonsgegevens door een gemeentelijke verwerkingsverantwoordelijke 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):
  beoordeling van een (voorgenomen) gegevensverwerking die waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen. In aanvulling op de beoordeling bevat een DPIA maatregelen om genoemd risico te verminderen of weg te nemen.
- Gegevenseigenaar:
  degene die *materieel* verantwoordelijk is voor de persoonsgegevens die binnen zijn taakgebied worden verwerkt. T.a.v. de gemeente Beemster zijn dat de teammanagers en de griffier.
- Informatiebeveiligingsdienst (IBD):
  De IBD is een onderdeel van de VNG. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy.
- Meldpunt datalekken:
  behandelaar van datalekken. Het meldpunt wordt bemenst door de CISO, de plv. CISO, de FG en de PO.
- Privacy:
  informationele privacy ofwel bescherming van persoonsgegevens.
- Privacyambassadeur:
  de "vooruitgeschoven post" op het gebied van privacy binnen een team en de intermediair tussen de FG/PO en de medewerkers van een team.

- PrivacyFunctionaris (PO):
  adviseur en ondersteuner van gegevenseigenaren op het gebied van privacy(wetgeving); bijvoorbeeld bij het opstellen van verwerkersovereenkomsten.
- Verwerkingsverantwoordelijke:
  degene die *formeel* verantwoordelijk is voor de persoonsgegevens die binnen zijn taakgebied worden verwerkt. Binnen de gemeente Beemster zijn dat: de gemeenteraad, het college van burgemeester en wethouders, de burgemeester, de heffingsambtenaar, de ambtenaar burgerlijke stand, de leerplichtambtenaar en de toezichthouder Wmo.

Deel 1 Terugblik op 2019; Borging, successen en (terechte?) zorgen

1.1 Toelichting titel

In het jaarverslag 2018 kwamen de volgende passages voor:

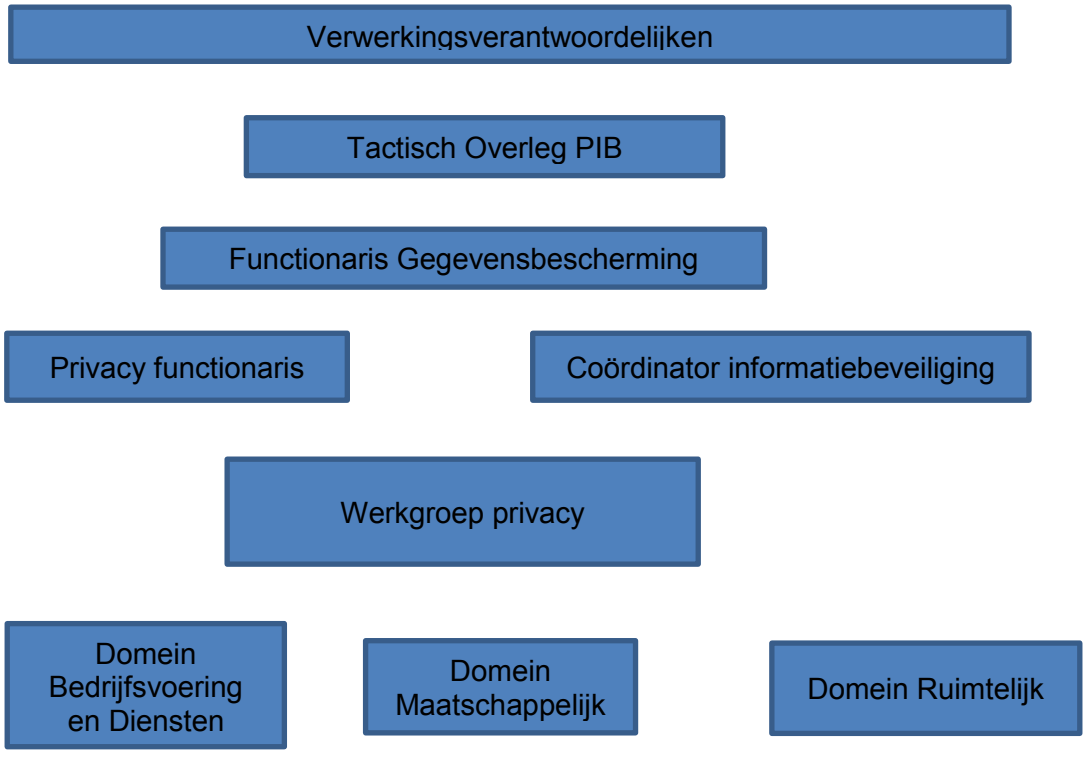
> *Waar de eerste Nederlandse AVG-golf zich kenmerkte door hectiek en deels door "window-dressing", kenmerkt de tweede AVG-golf zich door het besef dat privacy geen onderwerp is dat "wel weer overwaait" en daarom structurele borging vereist in de organisatie.*
>
> *Het is aan de gemeentelijke organisatie 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*.

In dit jaarverslag een weergave van wat de FG in 2019 gezien heeft van borging van de AVG in de raads- en college-organisatie, welke successen daarbij gevierd mogen worden, maar ook waar nog steeds – terecht of onterecht - zorgen over geuit worden.

1.2 Borging

1.2.1. Borging, de theorie

Voldoende aandacht voor privacy vereist allereerst dat vooraf is bepaald wie welke rol heeft bij dit onderwerp.
In het privacybeleid van de gemeente Beemster is het volgende overzicht opgenomen:



Naast het beleggen van de verschillende rollen, is een goed functionerende privacy-organisatie afhankelijk van de volgende randvoorwaarden:

- de verwerkingsverantwoordelijken (en de directie) hebben beleids- en procesmatige voorwaarden geschapen;

- de verwerkingsverantwoordelijken (en de directie) spreken hun commitment m.b.t. het onderwerp uit en tonen dit commitment middels:
  - het ter beschikking stellen van voldoende/doorlopende aandacht, geld en middelen;
  - het in positie brengen van de gegevenseigenaren;
  - het in positie brengen van FG en PO;
- de gegevenseigenaren vervullen hun rol als spil binnen de privacy-organisatie:
  - richting directie en verwerkingsverantwoordelijken;
  - richting FG en PO;
  - én richting hun medewerkers;
  - zij hebben oog voor de rol van de privacyambassadeurs binnen een team;
- de privacyambassadeurs kennen hun rol en nemen hun positie binnen hun team in;
- medewerkers:
  - kunnen in een privacy-vriendelijke omgeving werken;
  - kunnen met privacy-vriendelijke apparatuur werken;
  - kunnen zonder belemmeringen en consequenties signalen over privacy gerelateerde onderwerpen uiten, zowel richting de gegevenseigenaren áls richting de FG;
  - worden op de hoogte gehouden van nieuwe privacy-maatregelen die genomen zijn vanuit de verwerkingsverantwoordelijke, de directie en/of de gegevenseigenaar.

Borgingsinstrumenten[1] die het goed functioneren van een privacy-organisatie kunnen bevorderen of ondersteunen zijn:

- het hebben van actuele procesbeschrijvingen;
- het hebben en kennen van reglementen, modellen en good practices.
  Voorbeeld: model-verwerkersovereenkomst VNG, DPIA-tool IBD, lokale model-besluiten rechten betrokkenen;
- voor iedereen[2] toegankelijke communicatie over privacy-revelante onderwerpen.
  Voorbeeld: aparte privacypagina op de gemeentelijke website respectievelijk op intranet, berichten met privacy-actualiteiten op intranet, - op maat gesneden - presentaties voor medewerkers;
- toepassen privacy by design.
  Voorbeeld: juiste autorisaties, plekken om privacygevoelige stukken op te bergen, systemen die zicht geven op de mate van AVG-proof zijn van de organisatie.

1.2.2 Borging, de praktijk

Sinds de vaststelling van het privacybeleid op 29 mei 2018 heeft het overzicht op pagina 6 verder invulling gekregen:

- Wanneer nodig overleggen griffier[3] en FG over privacygerelateerde onderwerpen c.q. vraagt de griffier de FG om advies en ondersteuning;
- De FG is op 8 mei 2018 aangewezen en bekleedt deze functie voor 32 uur per week;
- In november 2018 is voor 16 uur per week een PO benoemd bij Juridische en Veiligheidszaken;
- Zomer 2019 is de formatie voor Informatiebeveiliging uitgebreid met een ISO; deze is per 1 maart 2020 aangesteld. Per 1 januari 2020 is – als opvolger van de Coördinator informatiebeveiliging - een CISO benoemd;
- Er zijn twee privacywerkgroepen actief waarin de privacyambassadeurs zitting nemen: de werkgroep Sociaal Domein, die nu uitgroeit tot de werkgroep Maatschappelijk Domein, en de algemene werkgroep waarin teams vertegenwoordigd kunnen worden die op andere taakvelden dan het Maatschappelijk Domein werkzaam zijn;

[1] Zowel landelijk (AP, VNG/IBD), regionaal als lokaal ontwikkeld c.q. bestaand

[2] Zowel medewerkers als betrokkenen

[3] M.b.t. de raads-organisatie neemt de griffier de plaats van het Tactisch Overleg in

- In de zomer van 2019 is het besluit genomen om de teammanagers aan te wijzen als gegevenseigenaren.

In de paragrafen 1.3.3 en 1.4 wordt verder ingegaan op de stand van zaken omtrent de in paragraaf 1.2.1 genoemde randvoorwaarden en instrumenten.

1.3 Successen en actiepunten

1.3.1 Successen uit 2018; stand van zaken

In het jaarverslag 2018 werden op de pagina's 6 en 7 de successen genoemd die gerelateerd waren aan het gemeentelijk privacybeleid:

1. het vaststellen van het gemeentelijk privacybeleid;
2. het aanwijzen van de FG;
3. het opstellen en bijhouden van een register datalekken;
4. het vormgeven van de processen rondom de rechten van betrokkenen;
5. het inrichten van de intranetpagina Privacy & Informatiebeveiliging (PIB-space);
6. het inrichten van de internetpagina Privacy;
7. het opzetten van privacywerkgroepen.

Wat is de stand van zaken met betrekking tot deze successen?

Ad 1. <u>Vaststellen van het gemeentelijk privacybeleid</u>

- Inmiddels is het gemeentelijk privacybeleid bijna twee jaar oud.
  (In ieder geval) qua terminologie kan het op onderdelen geactualiseerd worden.
- In het hoofdstuk Naleving, monitoring en evaluatie wordt een periodiek/jaarlijks vast te stellen actieprogramma vermeld.
  Dit actieprogramma is tot op heden niet gemaakt.
- Sinds november 2019 voert de FG gesprekken met de gegevenseigenaren over de stand van zaken omtrent privacy binnen hun team. Deze gesprekken worden gevoerd aan de hand van een borgingsdocument[4]. (zie bijlage)
  Op 9 maart 2020 heeft een eerste borgingsdocument-gesprek met de griffier plaatsgevonden.
  Diverse gegevenseigenaren geven aan het gemeentelijk privacybeleid uit te willen werken voor hun team (al dan niet in de vorm van concrete werkinstructies). Met één gegevenseigenaar zijn de gesprekken hierover in 2020 gestart.

Ad 2. <u>Aanwijzen van de FG</u>
In paragraaf 1.6 meer over de FG.

Ad 3. <u>Opstellen en bijhouden van een register datalekken</u>
Dit register is in 2018 opgesteld en wordt door het Meldpunt Datalekken permanent actueel gehouden.
In paragraaf 1.5 meer over datalekken.

Ad 4. <u>Vormgeven van processen rondom de rechten van betrokkenen</u>

- Op de privacypagina op de gemeentelijke website staan:
  - zes modelbrieven, die betrokkenen kunnen gebruiken als ze een recht geldend willen maken.
    In ieder geval behoeft de modelbrief inzageverzoek actualisatie a.h.v. jurisprudentie.
  - de contactgegevens van de FG en de AP.
    Deze gegevens zijn actueel.
- Op de intranetpagina "privacy en informatiebeveiliging" staan de bij de 6 modelbrieven behorende modelbesluiten.

[4] Dit document is geënt op het VNG-document "Borging AVG, Het borgen van de AVG in de gemeentelijke organisatie".

In ieder geval behoeft het modelbesluit inzageverzoek actualisatie a.h.v. jurisprudentie.

- Op de intranetpagina “procesbeschrijvingen” staat het proces: afhandelen inzageverzoek persoonsgegevens.
  - Uit de borgingsdocument-gesprekken blijkt dat het merendeel van de gegevenseigenaren deze procesbeschrijving niet kent.
  Op een enkele uitzondering na, geven de gegevenseigenaren ook aan dat zij geen behoefte hebben aan procesbeschrijvingen voor de andere rechten van betrokkenen. Dit oordeel wordt mede ingegeven door het feit dat m.b.t. hun teams betrokkenen nauwelijks een beroep doen op deze rechten.
  - Net als de modelbrief en het modelbesluit, behoeft de procesbeschrijving inzageverzoek actualisatie a.h.v. jurisprudentie.
  - Aan de directie heeft de FG inmiddels geadviseerd het maken van procesbeschrijvingen m.b.t. de andere 5 rechten van betrokkenen in 2020 toch in gang te zetten, te beginnen bij de rechten tot rectificatie en wissing. Het op orde hebben van processen en procesbeschrijvingen, ook al komen ze in de praktijk niet frequent voor, is een borgingsvereiste in het kader van de AVG.

Ad 5. Inrichten van de intranetpagina Privacy & Informatiebeveiliging
In het jaarverslag 2018 had dit item als toelichting dat de intranetpagina in 2019 een professionaliseringsslag zou ondergaan. Deze slag is tot op heden niet afgerond.

Ad 6. Inrichten van de internetpagina Privacy
Met inachtneming van het hierboven gestelde over de modelbrieven en het register van verwerkingsactiviteiten, wordt deze pagina actueel gehouden.

Ad 7. Opzetten van privacywerkgroepen
Privacywerkgroepen kunnen alleen vergaderen als gegevenseigenaren privacyambassadeurs hier naar afvaardigen. Inmiddels bestaat de algemene werkgroep uit 15 leden met vertegenwoordigers uit het Ruimtelijk Domein, uit Bedrijfsvoering en uit de griffie.

Samenvattend is de volgende vergelijking tussen 2018 en 2019 te maken [5]

		2018	2019
1.	**Vaststellen (onderhouden en uitwerken) privacybeleid**		
2.	**Aanwijzen (en in positie brengen/houden) FG** (zie ook § 1.6)		
3.	**Opstellen en bijhouden register datalekken**		
4.	**Vormgeven proces rechten betrokkenen**		
5.	**Inrichten en onderhouden intranetpagina Privacy & Informatiebeveiliging (PIB-space)**		
6.	**Inrichten en onderhouden internetpagina Privacy**		
7.	**Opzetten en continueren privacywerkgroepen**		

1.3.2. Actiepunten uit 2018; stand van zaken
In het jaarverslag 2018 werden op de pagina’s 6 en 7 de actiepunten opgesomd die gerelateerd waren aan het gemeentelijk privacybeleid:

1. het opstellen van een register van verwerkingsactiviteiten;
2. de aantoonbaarheid van verkregen toestemming;
3. het beoordelen van de rechtmatigheid van gegevensverwerkingen;
4. het afsluiten van verwerkersovereenkomsten;
5. het stimuleren van de privacycultuur/voeren privacybewustwordingscampagnes;

[5] Verklaring kleuren in tabel: groen = afgeronde actie; oranje = actie opgepakt, nog niet afgerond; rood = actie nog niet opgepakt

6. het implementeren van organisatorische privacy by design;
7. het opstellen van procesbeschrijvingen.

Wat is de stand van zaken m.b.t. deze actiepunten?

Ad 1. Opstellen en onderhouden van een register van verwerkingsactiviteiten
Sinds februari 2018 wordt het register van verwerkingsactiviteiten vormgegeven en gevuld. Door team Communicatie is in 2019 een gebruiksvriendelijk register ontworpen. Dit register bevat nu bijna 170 unieke verwerkingen van de verwerkings-verantwoordelijken van Beemster (al dan niet samen met de verwerkingsverantwoordelijken van Purmerend). De gemeenteraad van Beemster kent 1 eigen verwerking: de onteigeningsprocedure en 22 verwerkingen met een gedeelde verantwoordelijkheid met college en/of burgemeester.
De FG en de PO hebben o.g.v. het privacybeleid de tekstuele eindredactie van het register. Tijdens de borgingsdocument-gesprekken worden de gegevenseigenaren er op gewezen dat zij inhoudelijk verantwoordelijk zijn voor de verwerkingen die onder hun verantwoordelijkheid vallen. Hiermee zijn zij verantwoordelijk voor het doorgeven van wijzigingen in deze verwerkingen die consequenties voor het register hebben. Hiermee zijn zij óók verantwoordelijk voor bijvoorbeeld het afsluiten van verwerkersovereenkomsten daar waar een verwerker wordt ingeschakeld.
In 2019 hebben de FG en de PO vanuit de griffie geen verzoeken gehad tot actualisering van verwerkingen waarvoor de raad (mede) verantwoordelijk is.
Uit zijn aard is dit een permanent actiepunt.

Ad 2. Aantoonbaarheid van verkregen toestemming
Door de FG is hier in 2019 niet separaat aandacht voor gevraagd of controle op uitgeoefend. Team Belastingen heeft op eigen initiatief een formulier (kwijtschelding) ontwikkeld waarmee toestemming kan worden aangetoond.

Ad 3. Beoordelen rechtmatigheid gegevensverwerkingen
Door de FG is hier in 2019 - door omstandigheden - niet separaat aandacht voor gevraagd of controle op uitgeoefend.

Ad 4. Afsluiten van verwerkersovereenkomsten
Door Coördinatie Aanbesteding en Juridische en Veiligheidszaken worden gegevenseigenaren er zoveel mogelijk op gewezen om bij nieuwe contracten – waar nodig – ook een verwerkersovereenkomst af te sluiten.
Waar bij de 23 verwerkingen waar de raad (mede) verantwoordelijk voor is een verwerker is ingeschakeld, zijn voor 22 verwerkingen ook daadwerkelijk verwerkersovereenkomsten afgesloten[6].

Ad 5. Stimuleren privacycultuur/voeren privacybewustwordingscampagnes
De privacywerkgroepen, de borgingsdocument-gesprekken en de presentaties voor het personeel zijn voorbeelden van instrumenten om het privacybewustzijn te vergroten.
Uit zijn aard is dit een permanent actiepunt.

Ad 6. Implementeren organisatorische privacy by design
In de paragrafen 1.3.3 en 1.4 wordt de stand van zaken m.b.t. dit onderwerp verder toegelicht.

Ad 7. Opstellen procesbeschrijvingen
Zie paragraaf 1.3.1, onder 4.

[6] De gegevenseigenaar wordt gevraagd voor de 23e verwerking (einde dienstverband op verzoek werkgever/van rechtswege) alsnog een verwerkersovereenkomst af te sluiten.

Samenvattend is de volgende vergelijking tussen 2018 en 2019 te maken

		2018	2019
1.	**Opstellen en onderhouden register van verwerkingsactiviteiten**		
2.	**Daar waar toestemming de grondslag voor gegevensverwerking is, kunnen aantonen dat toestemming is gegeven**		
3.	**Beoordelen rechtmatigheid gegevensverwerkingen**		
4.	**Afsluiten verwerkersovereenkomsten**		
5.	**Stimuleren privacycultuur/voeren privacybewustwordings-campagnes**		
6.	**Implementeren organisatorische privacy by design**		
7.	**Opstellen procesbeschrijvingen**		

1.3.3 Successen uit 2019

De volgende zaken zijn specifiek in 2019 als een succes te bestempelen:

- Reglementen, modellen en good practices:
  - Op 23 oktober 2019 is het Reglement veilig gegevensgebruik en privacy gemeente Purmerend 2019 in werking getreden. Beemster heeft dit reglement in januari 2020 vastgesteld.
  Dit reglement kan (mede) worden beschouwd als concretisering van het privacybeleid en is ook van toepassing op griffiemedewerkers.
- Voor iedereen toegankelijke communicatie over privacy-relevante onderwerpen:
  - sinds de zomer van 2019 worden alle nieuwe medewerkers uitgenodigd voor een AVG-presentatie;
  - afspraken zijn gemaakt om voor alle medewerkers op De Koog op maat gemaakte privacypresentaties te geven via zgn. toolboxen. Hiermee is in maart 2020 daadwerkelijk gestart.
- Toepassen privacy by design
  - Via de gegevenseigenaren kunnen medewerkers die gevoelige persoonsgegevens verwerken een sleutel krijgen voor hun werkkastje;
  - Sinds eind 2019 zijn de verzamelafvakbakken in de vergaderruimtes van het stadhuis van Purmerend, in de reuringruimtes en in (diverse) regelmaatruimtes niet langer bestemd voor papier. Papier wordt nu ingezameld via de afgesloten papiercontainers die naast de printers in de reuringruimtes staan;
  - In december 2019 start een proef met 2 belcellen, waarin geluidsdicht gebeld kan worden;
  - sinds maart 2020 heeft Purmerend een Privacymanagementsysteem. Dit systeem gaat ingezet worden om de privacy-PDCA-cyclus beter te kunnen beheersen;
  - bij alle printers, óók op De Koog, is sinds oktober 2019 de automatische uitlogtijd ingesteld op 20 seconden.

1.4 Zorgen

1.4.1 Zorgen/signalen medewerkers

Ook in 2019 hebben medewerkers signalen naar voren gebracht c.q. zorgen geuit over de verwerking van persoonsgegevens op het stadhuis; mede t.b.v. de gemeente Beemster. Hieronder een opsomming voor zover (ook) relevant voor de gemeenteraad.

	Onderwerp signaal	**2018**	**2019**
1.	Openheid reuring-, regelmaat- en vergaderruimtes stadhuis	X	X
2.	Voor iedereen toegankelijke open papiercontainers achter het stadhuis	X	X
3.	Inzage geven in elkaars gevoelige dossiers	X	X

4.	Mee binnen laten van onbekende personen door de achterdeur	X	X
5.	Weglopen bij printer als opdracht nog niet voltooid is		X

Toelichting signalen
1. Openheid reuring-, regelmaat- en vergaderruimtes stadhuis
- Op pagina 11 is de proefopstelling van belcellen als – potentieel - succes genoemd en als mogelijkheid om een deel van de zorgen van medewerkers weg te nemen.
- De FG gaat monitoren in hoeverre de implementatie van het Reglement veilig gegevensgebruik en privacy een (verdere) verbetering brengt in de manier waarop medewerkers met deze openheid om (moeten) gaan.
2. Voor iedereen toegankelijke open papiercontainers achter het stadhuis
Medewerkers, maar ook de FG baart deze situatie zorgen. Dankzij intensieve interventie van de (plv) CISO lijkt in deze situatie eind 2019 een kentering ten goede te komen.
3. (inzage geven in elkaars gevoelige dossiers), 4. (mee naar binnen laten van onbekende personen door de achterdeur)
Ten opzichte van de situatie in 2018 is – gezien de binnengekomen klachten - op deze punten onvoldoende verbetering opgetreden. Gezien het feit dat punt 4 mede bepalend is voor de (privacy)veiligheid in de rest van het stadhuis, zal hier in 2020 extra op gelet moeten worden.
5. Weglopen bij printer als opdracht nog niet voltooid is
Printers kunnen een hun gegeven opdracht niet uitvoeren als bijvoorbeeld de papierlade of de toner leeg is. Zodra het papier aangevuld of de toner vervangen is worden eerder gegeven opdrachten alsnog geprint. Regelmatig krijgen medewerkers én externen daardoor stukken/persoonsgegevens onder ogen die niet voor hen bestemd zijn. Dit levert datalekken op. Het is daarom zaak medewerkers er op te wijzen dat zij checken of hun hele opdracht is geprint en zo niet om maatregelen te nemen dat dit alsnog gebeurt.

1.4.2 Zorgen/klachten betrokkenen
De FG heeft in 2019 acht klachten van betrokkenen ontvangen. Deze betroffen allemaal persoonsgegevens die onder de verantwoordelijkheid van college of burgemeester verwerkt worden.

1.4.3 Zorgen FG, PO en privacyambassadeurs; voortdurende c.q. aanvullende knelpunten
In aanvulling op bovenstaande punten, vraagt de FG, mede op verzoek van de privacyambassadeurs, aandacht voor het volgende:
1. DPIA's
In het jaarverslag 2019 stonden 2 acties uit het privacybeleid "op rood": het beschikbaar hebben respectievelijk het uitvoeren van DPIA's.
Bij deze constatering stond de volgende toelichting:
"*Analyses, puur vanuit privacyperspectief, 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."

Inmiddels zijn we een jaar verder:
- De IBD heeft in juli 2019 een landelijke DPIA-tool online gezet;
- De AP heeft in november 2019 de definitieve verplichte-DPIA-lijst in de Staatscourant geplaatst,

maar:

- de tool van de IBD werkt in de praktijk niet naar behoren, waardoor de organisatie nog steeds zoekende is naar een goed DPIA-model;
- er is slechts één DPIA (vanuit het college Purmerend, óók t.b.v. Beemster) voor verplicht advies aan de FG voorgelegd.

Het uitvoeren van een DPIA wordt soms gezien als werkverschaffing aan de organisatie. Dit is het niet. Doel van een DPIA is om helder te krijgen welke risico's er aan een nieuwe verwerking/nieuw samenwerkingsverband/nieuw systeem kleven. Pas als helder is welke risico's er zijn, kunnen maatregelen genomen worden om deze risico's te ondervangen. Het is daarom van belang dat de verwerkingen die daarvoor in aanmerking komen aan een DPIA worden onderworpen.

Samenvattend blijven DPIA's het volgende beeld opleveren:

		2018	**2019**
1.	Beschikbaar hebben DPIA's		
2.	Uitvoeren DPIA's		

2. Overige knelpunten uit het jaarverslag 2018
Onderwerpen die in het jaarverslag 2018 werden aangekaart en waar ook in 2019 vragen bij gesteld kunnen worden:

- Ontbreken van kennis over een juiste verwerking van persoonsgegevens bij een deel van de medewerkers. Dit vergt – en deels: krijgt - permanente aandacht van de gegevenseigenaren.
- Ontbreken (regels voor) periodieke opschoning L-schijf en mailbox;
- Niet AVG-proof zijn van systemen.

3. Aanvullend knelpunt

- *Samenwerkingsverbanden*
  Buiten- of intergemeentelijke samenwerking is vaak noodzakelijk om gemeentelijke taken uit te kunnen voeren. Samenwerking kan veel gedaanten aannemen:
  1. samenwerking waarbij één partij de ander een dienst verleent door bepaalde taken uit te voeren. Denk aan het ter beschikking stellen van cloudopslag.
  2. samenwerking waarbij twee partijen gegevens uitwisselen om ieders taken uit te kunnen voeren. Denk aan de uitwisseling van persoonsgegevens tussen griffier en bedrijfsarts over een zieke medewerker.
  3. samenwerking waarbij twee of meer partijen via een gemeenschappelijk systeem gegevens uitwisselen om ieders taken uit te kunnen voeren. Denk aan samenwerking op het gebied van integrale veiligheid via de Veiligheidshuizen.
  4. Samenwerking waarbij meerdere partijen op basis van een gemeenschappelijke regeling een nieuw openbaar lichaam oprichten dat vervolgens als zelfstandige entiteit gegevens uitwisselt met de samenwerkende partijen. Denk aan het openbaar lichaam Recreatieschap Twiske.

  Kennis over de privacyrechtelijke consequenties van de verschillende vormen van samenwerking is noodzakelijk om de gegevensuitwisseling tussen de samenwerkende partijen in juiste banen te leiden. Niet alleen voor wat betreft de (wijze van) gegevensuitwisseling zelf, maar ook voor wat betreft de aan de uitwisseling ten grondslag liggende stukken zijn er verschillen.
  Samenwerking:
  1. Wordt vormgegeven middels een verwerkersovereenkomst;
  2. Kan worden vormgegeven middels een privacyconvenant, maar kan ook gewoon "organisch groeien" zonder concrete voorafgaande afspraken. De inhoud van het privacyconvenant is vormvrij;
  3. Moet worden vormgegeven middels een privacyconvenant. De inhoud van dit privacyconvenant wordt mede bepaald door de AVG;

4. Kan en soms: moet worden vormgegeven middels een privacyconvenant.

Geadviseerd wordt in 2020 aandacht aan dit onderwerp te gaan besteden, in ieder geval door te inventariseren in hoeverre de samenwerkingsverbanden waarin de gemeenteraad participeert privacyrechtelijk op orde zijn.

1.5 Meldpunt datalekken

De CISO, plv. CISO, FG en PO hebben in 2019 2 datalekken behandeld die (ook) onder de verantwoordelijkheid van de gemeenteraad vielen:

- Het eerste datalek (januari 2019) betreft het aan alle gegevenseigenaren sturen van een lijst met 550 terugbelverzoeken, inclusief vermelding N(AW)-gegevens bellers + korte omschrijving onderwerp. In deze omschrijving staan ook gevoelige gegevens, bijvoorbeeld m.b.t. een lopend Jeugdzorgtraject.
  Direct na ontdekking van het datalek heeft het versturende team alle gegevenseigenaren verzocht de betreffende lijst te vernietigen. Vervolgens is per gegevenseigenaar een nieuwe lijst verstuurd, met daarin alleen de terugbelverzoeken van zijn team.
- Het tweede datalek (maart 2019) betreft de open papiercontainers in het berghok aan de achterzijde van het stadhuis. (Rokende) medewerkers treffen in deze containers allerlei zeer gevoelige stukken/persoonsgegevens aan.
  Zoals aangegeven op pag. 12 lijkt deze situatie zich in de loop van 2019 te verbeteren.

Sinds 2018 hanteert de AP de richtlijn dat datalekken die zich binnen de “betrouwbare kring”[7] van de overheid afspelen niet gemeld hoeven worden. Daarom is geen van de datalekken gemeld aan de AP.

Aangezien er zich in 2018 geen datalekken hebben voorgedaan die onder de verantwoordelijkheid van de Beemster gemeenteraad vielen, is er in 2019 sprake van een kleine stijging. De FG heeft niet de indruk dat deze stijging te wijten is aan een slechtere omgang met persoonsgegevens. De stijging lijkt ook/vooral te maken te hebben met een grotere bewustwording t.a.v. het fenomeen datalekken en een betere bekendheid van het meldpunt.

1.6 “Team privacy”

Door (gedeeltelijke) uitval van de FG, is team privacy in 2019 gedurende meerdere maanden niet op volle sterkte. Dit heeft een zware wissel getrokken op de PO en de tijdelijke ondersteuner.
Zaken zijn hierdoor onvoldoende, te laat of niet opgepakt.

Voor zover het de FG betreft, is 2019 het laatste jaar dat Werkom binnen het takenpakket valt. Sinds 1 januari 2020 heeft Werkom een eigen FG aangetrokken. De FG’s van Zaanstad en Purmerend zijn inmiddels met deze FG in gesprek over de vormgeving van hun onderlinge samenwerking.

Nu de FG sinds 1 januari weer volledig inzetbaar is, zal in 2020 met de gemeentesecretaris van Purmerend het gesprek aangegaan worden over de toekomst van team privacy.

[7] Tot de betrouwbare kring behoren vertrouwde zakelijke relaties en personen met een beroepsgeheim, zoals eigen personeel en medici.

Deel 2 Vooruitblik naar 2020, consolideren

2.1 Voortzetten borging

De vooruitblik naar 2019 had de titel: Op weg naar borging.
Borging werd daarbij – conform het privacybeleid – als volgt omschreven:
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

In deel 1 is aangegeven hoe de gemeentelijke (privacy-)organisatie er voor staat.
Hieruit blijkt dat er stappen zijn gezet naar een betere borging van de privacywetgeving.
De FG blijft met de griffier in gesprek om deze borging te continueren en waar mogelijk te vergroten.

2.2 Acties

2.2.1 Permanente actiepunten

	Actiepunt	Toelichting	Planning
1.	beoordelen actualiteit + bijhouden register van verwerkingsactiviteiten	het register is de basis voor inzicht in gegevensverwerkingen; actueel houden is prioriteit 1 Van gegevenseigenaren/de griffier wordt verwacht dat zij hun verantwoordelijkheid hierin nemen	Permanente actie
2.	beoordelen rechtmatigheid gegevensverwerkingen		"
3.	Monitoren aanwezigheid privacyconvenant bij gezamenlijk verwerkingsverantwoordelijken	De verplichting hiertoe is neergelegd in artikel 26 AVG	
4.	onderhouden en waar nodig versterken privacybewustzijn	de FG speelt hier een actieve rol, o.a. via het geven van presentaties en het voorzitterschap van de privacy-werkgroepen	"
5.	monitoren vormgeven organisatorische privacy by design	met actiepunt 6 vormt dit punt de basis voor medewerkers om privacyproof te kúnnen werken	"
6.	monitoren vormgeven privacy by design in systemen	dit punt wordt in samenwerking met de CISO (en waar mogelijk/nodig met externe organisaties) opgepakt	"
7a.	monitoren uitvoeren DPIA's	Dit vindt plaats a.h.v. de verplichte DPIA-lijst van de AP	"
7b.	adviseren m.b.t. DPIA's	concept-DPIA's worden verplicht ter advisering aan de FG voorgelegd	"
8.	up to date houden internet pagina privacy en PIB space op intranet	Dit is een gezamenlijke verantwoordelijkheid van de FG en de PO, en voor zover het de PIB space betreft tevens van de (C)ISO	"
9.	afhandelen klachten betrokkenen	Betrokkenen kunnen zowel burgers als medewerkers zijn	"
10.	houden borgingsdocument-gesprekken met de griffier	Dit vindt plaats a.h.v. bijgevoegd borgingsdocument	"

2.2.2. Incidentele actiepunten

	Actiepunt	Toelichting	Planning
1.	beoordelen rechtmatig toepassen grondslag toestemming	opgepakt als onderdeel van structureel actiepunt 2	Vanaf K2
2.	monitoren actualiseren procesbeschrijving afhandelen inzageverzoek	actualisatie vloeit voort uit nieuwe jurisprudentie	Vanaf K3
3.	beoordelen aanwezigheid overige procesbeschrijvingen inzake rechten betrokkenen	Dit punt vloeit voort uit het op pag. 9 gegeven advies aan de directie	Vanaf K3
4.	Monitoren privacyaspecten Omgevingswet	Mede a.h.v. de DPIA 2019 DSO en Omgevingswet	Vanaf K4[8]
5.	(met Communicatie) verbeteren zichtbaarheid FG voor burgers en betrokkenen		Vanaf K3
6.	Monitoren effecten Reglement veilig gegevensgebruik en privacy	Monitoring zal plaatsvinden nadat de CISO en de PO alle teams hebben geïnformeerd over het Reglement	Vanaf K3

[8] Wanneer duidelijkheid bestaat omtrent de (wederom uitgestelde) inwerkingtreding van de Omgevingswet

Bijlage 1 Borging van de AVG in tabelvorm[1]

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 de omgang met persoonsgegevens van medewerkers en bestuursleden					
Wordt periodiek getoetst en waar nodig geactualiseerd					
Privacyverklaring is gepubliceerd op de website					(X)
Bezoekers van de gemeentelijke website worden geïnformeerd over cookies					

[1] 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.

De FG

Activiteiten	onbekend/(nog) niet van toepassing	ontbreekt	onvoldoende/niet gemeentebreed	voldoende	goed/afgerond
Verwerkingsverantwoordelijken hebben een FG aangewezen					X
Het is voor medewerkers duidelijk wie de FG is en wat zijn taken zijn					
De FG wordt om advies en ondersteuning gevraagd bij bewustwording privacy binnen de organisatie					
De FG wordt – in ieder geval door de gegevenseigenaren - tijdig betrokken bij zaken die verband houden met privacy					
De FG beschikt over de middelen + toegangen tot gegevens die nodig zijn 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 over de omgang met persoonsgegevens binnen de organisatie					X

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/werkterrein					

Activiteiten	onbekend/(nog) niet van toepassing	ontbreekt	onvoldoende/niet gemeentebreed	voldoende	goed/afgerond
Er zijn privacy-ambassadeurs binnen de teams aangewezen die dienen als aanspreekpunt voor directe collega's					
De privacy-ambassadeurs bespreken periodiek met de FG en de privacyfunctionaris landelijke ontwikkelingen, vragen uit de organisatie en andere privacy-gerelateerde onderwerpen					

Processen

Activiteiten	onbekend/(nog) niet van toepassing	ontbreekt	onvoldoende/ niet gemeentebreed	voldoende	goed/afgerond
Er zijn processen/procesbeschrijvingen en voorzieningen voor het faciliteren van de rechten van betrokkenen					
De OR wordt actief geïnformeerd over dan wel om instemming gevraagd over privacy en gegevensbescherming voor wat betreft het personeel					X
Externen tekenen bij aanvang van hun werkzaamheden voor de organisatie een integriteits- en geheimhoudingsverklaring					
Inzichtelijk is welke besluiten genomen worden op basis van geautomatiseerde besluitvorming					
Nieuwe verwerkingen c.q. processen/systemen wordt ingericht volgens het principe van privacy by design/privacy by default c.q. worden tijdig getoetst aan privacywetgeving					

Activiteiten	onbekend/(nog) niet van toepassing	ontbreekt	onvoldoende/ niet gemeentebreed	voldoende	goed/afgerond
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/de omgang met persoonsgegevens 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 gemeentelijke bestuursorganen (gezamenlijk) verwerkingsverantwoordelijke zijn					
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 door de privacyfunctionaris en de FG					X
Gegevenseigenaren zijn verantwoordelijk voor het register en geven nieuwe verwerkingen/wijzigingen van bestaande verwerkingen door aan de beheerders van het register					

DPIA's

Activiteiten	onbekend/(nog) niet van toepassing	ontbreekt	onvoldoende/niet gemeentebreed	voldoende	goed/afgerond
Bij gegevenseigenaren is bekend wie een DPIA uitvoert					
Bij nieuwe verwerkingen of de aanschaf van nieuwe systemen is in beeld of deze een hoog privacyrisico hebben en zo ja, wordt een DPIA uitgevoerd					
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 m.b.t. een DPIA					
Resultaten van DPIA's zijn geregistreerd (in het register van verwerkingsactiviteiten) en worden teruggekoppeld naar de betrokken medewerkers					
Op basis van DPIA's uit te voeren maatregelen worden uitgevoerd					
DPIA's worden periodiek – minimaal elke 3 jaar – herhaald. Ten behoeve hiervan is er een overzicht van uitvoerdata van gehouden DPIA's.					

Noodzakelijke kennis bij medewerkers

Activiteiten	onbekend/(nog) niet van toepassing	ontbreekt	onvoldoende/niet gemeentebreed	voldoende	goed/afgerond
Medewerkers zijn op de hoogte van het bestaan van het register van verwerkingsactiviteiten					
Alle medewerkers zijn op de hoogte van hun algemene geheimhoudingsplicht					
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 (waarbij gebruik wordt gemaakt van de modelbrieven) en het juist gebruik van grondslagen voor verwerking (m.n. de grondslag: toestemming)					
Medewerkers weten wat datalekken zijn en 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					

Activiteiten	onbekend/(nog) niet van toepassing	ontbreekt	onvoldoende/niet gemeentebreed	voldoende	goed/afgerond
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					

Activiteiten	onbekend/(nog) niet van toepassing	ontbreekt	onvoldoende/niet gemeentebreed	voldoende	goed/afgerond
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 door de gegevenseigenaar tijdig passende afspraken gemaakt; deze worden vastgelegd in een verwerkersovereenkomst dan wel privacyconvenant					
Een eenmalige gegevensuitwisseling met een externe partij is AVG-proof; indien nodig worden hierover schriftelijke afspraken gemaakt					

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