

**JAARVERSLAG FUNCTIONARIS GEGEVENSBESCHERMING
GEMEENTE BEEMSTER 2020**

Gemeenteraad

Over corona en privacy (in de verdrinking?)

12 april 2021

VOORWOORD

2020: twee jaar AVG, maar vooral het jaar waarin de wereld op zijn kop staat vanwege het coronavirus.

Het virus trekt ook op de medewerkers van de gemeenten Purmerend en Beemster en op de omstandigheden waaronder ze moeten (thuis)werken een zware wissel. Dit heeft soms ook effect op de manier waarop de privacywetgeving wordt uitgevoerd.

Ik wil u als lezer meenemen door het privacy jaar 2020 en hoop hiermee een beeld te geven van hoe Beemster er vanuit – mijn - privacy perspectief voor staat.

Ik ga graag met u in gesprek over dit verslag.

Purmerend, 12 april 2021

INHOUDSOPGAVE

Samenvatting	4
Verklarende woordenlijst	4
Deel 1 Terugblik op 2020	
1.1 2019 vervolgd	6
1.2 Privacy in cijfers	6
1.2.1. De cijfers	6
1.2.2. De cijfers toegelicht	6
1. Zorgen/klachten betrokkenen	6
2. Zorgen/signalen medewerkers	7
3. DPIA's	8
4. Datalekken	8
1.3 Actielijst uit jaarverslag 2019, stand van zaken	8
1.4 Wat viel verder op in 2020	11
1.4.1. uit het borgingsdocumentgesprek	11
1.4.2. overige onderwerpen	11
1. Brexit en Privacyshield	11
2. Algoritmes en A(rtificial) I(ntelligence)	11
3. Verwerkers, aandachtspunten en (wan)gedrag	12
4. Ondernijning	12
5. Kaderbrief	13
6. Privacygerelateerde effecten van corona	13
Deel 2 Vooruitblik naar 2021; fusiejaar	
2.1 Privacyproof fuseren tijdens een pandemie	14
2.2 Acties	14

Samenvatting

2 Jaar AVG, maar geen business as usual. Corona verandert de manier van werken ingrijpend en vertraagt op plekken het AVG-borgingsproces. Het brengt het echter niet tot stilstand en er zijn zelfs ook ronduit positieve privacy-ontwikkelingen.

Een opsomming van zaken:

- Er wordt een privacyadviseur aangenomen bij Juridische Zaken en het aantal privacyambassadeurs blijft stijgen. Ook de griffie krijgt dit jaar een eigen – actieve - privacyambassadeur;
- Teams geven zelf aan behoefte te hebben aan informatie ter bevordering van het privacybewustzijn bij nieuw maar ook bij zittend personeel;
- Op De Koog start een facilitymanager die deze locatie meer in overeenstemming met de privacywetgeving moet brengen;
- Het merendeel van de door burgers bij de FG ingediende privacyklachten blijkt ongegrond;
- Een flink deel van de door medewerkers geuite signalen wordt opgepakt;
- Zorgenkindje blijven de DPIA's, ook in 2020 wordt er niet één vastgesteld. Hierdoor blijven risico's die gepaard gaan met nieuwe verwerkingen of met de aanschaf van nieuwe systemen onderbelicht;
- De nieuwe privacyambassadeur gaat hard aan de slag om de verwerkingen van persoonsgegevens door de griffie in het register van verwerkingsactiviteiten te krijgen;
- Het blijft lastig om samenwerkingsverbanden inzichtelijk te krijgen. Dit heeft ook een effect op het soepel verlopen van het fusieproces;
- Algoritmes en AI zullen hun opmars in de gemeentelijke praktijk voortzetten. Het is belangrijk dat college én raad aangeven – ieder voor zover het hun eigen terrein betreft - wat hierin acceptabel is;
- De aanpak van ondermijning gaat met het instellen van een Team Ondermijning een nieuwe fase in. Juist bij ondermijning is het permanent stellen van privacy-gerelateerde vragen onontbeerlijk.

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): hoogste 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/"third line of defense" 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. Binnen de gemeenten Beemster en Purmerend zijn dat de teammanagers en de griffiers.
- Meldpunt datalekken:
behandelaar van datalekken. Het meldpunt wordt bemenst door de CISO, de PO, de FG (eerste helft van het jaar), de ISO (tweede helft van het jaar), de privacyadviseur (tweede helft van het jaar).
- PIB:
verzamelnaam voor de PO, privacyadviseur, FG, CISO en ISO en de onderwerpen: Privacy en InformatieBeveiliging
- Privacy:
informationele privacy ofwel bescherming van persoonsgegevens.
- Privacyadviseur:
adviseur en ondersteuner van gegevenseigenaren op het gebied van privacy(wetgeving); o.a. bij het opstellen van verwerkersovereenkomsten en het beheren van het Register van verwerkingsactiviteiten.
- Privacyambassadeur:
de “vooruitgeschoven post”/“first line of defense” en de intermediair tussen de FG/PO en de medewerkers van een team op het gebied van privacy binnen een team.
- PrivacyFunctionaris (PO):
adviseur/“second line of defense” en ondersteuner van gegevenseigenaren op het gebied van privacy(wetgeving); o.a. bij het uitvoeren van DPIA's.
- Verwerkingsverantwoordelijke:
degene die *formeel* verantwoordelijk is voor de persoonsgegevens die binnen zijn bevoegdheidsfeer worden verwerkt. Binnen de gemeente Beemster zijn dat: het college van burgemeester en wethouders, de gemeenteraad, de burgemeester, de heffings- en invorderingsambtenaar, de ambtenaar burgerlijke stand, de leerplichtambtenaar en de toezichthouder Wmo.

Deel 1 Terugblik op 2020; corona en privacy (in de verdrinking?)

1.1. 2019 vervolgd

Het jaarverslag over 2019 sloot af met de constatering dat er stappen zijn gezet naar een betere borging van de privacywetgeving door de gemeentelijke organisatie. Dit jaarverslag gaat verder waar het vorige eindigde.

Wat valt er dan direct op in 2020:

- In september 2020 start bij Juridische Zaken naast de PO, een privacyadviseur;
- Het aantal privacyambassadeurs groeit gestaag. Eind december staat de teller op 29 (en bij het schrijven van dit jaarverslag op 34). Ook de griffie krijg in 2020 een eigen privacyambassadeur;
- De griffie levert de eerste set verwerkingen aan t.b.v. het register van verwerkingsactiviteiten.
- De FG heeft vaste overleggen met teams waar zeer gevoelige persoonsgegevens worden verwerkt dan wel belangrijke ontwikkelingen gaande zijn.
Voorbeeld van het eerste: het overleg met Team Integrale Veiligheid (TIV);
Voorbeeld van het laatste: het overleg met verschillende teams over algoritmes en AI.

En wat valt er verder te zeggen over 2020, gezien vanuit privacy perspectief.

1.2 Privacy in cijfers

1.2.1 De cijfers

	Onderwerp	2018	2019	2020
1.	Zorgen/klachten betrokkenen	3	8	11
2.	Zorgen/signalen van medewerkers	20	31	16
3.	DPIA's	0	0	0
4.	Datalekken raad	0	2	0

1.2.2. De cijfers toegelicht

1. Zorgen/klachten betrokkenen

De FG heeft in 2020 11 klachten van betrokkenen ontvangen m.b.t. de verwerking van hun persoonsgegevens. Hieronder bevinden zich ook 2 klachten van (oud) medewerkers (van Purmerend).

5 Klachten zijn (deels) terecht, althans voor zover het Beemster en Purmerend betreft.

De klachten betreffen de volgende onderwerpen:

- gebruik van BSN als ware het een KvK nummer ((on)terechte klacht. Er zijn geen signalen dat deze situatie zich momenteel in Beemster voordoet. Bij andere overheidsorganisaties komt dit wél voor.)
- versturen belastingaanslagen naar verkeerd adres (onterechte klacht)
- versturen persoonslijsten in ondeugdelijke envelop (terechte klacht)
- verstrekken persoonsgegevens uit Brp aan advocaat (onterechte klacht)
- opgelegde verplichting kopie paspoort via niet beveiligde mailverbinding te versturen (terechte klacht)

- team Veiligheid gebruikt contactgegevens betrokkene om te hacken (onterechte klacht. Blijkt een externe te zijn die zich voordoeft als medewerker van het team)
- openbare orde camera Koemarkt filmt in woningen betrokkenen (terechte klacht)
- persoonsgegevens in stukken bezwaarprocedure gedeeld met andere belanghebbenden (grotendeels onterechte klacht)
- (etnische) gegevens van derden aangetroffen in eigen PD (onterechte klacht)
- eigen PD is onvolledig (terechte klacht)
- aan een verzoek om rectificatie van een Wmo indicatie wordt geen uitvoering gegeven (klachtafhandeling gestopt doordat betrokkene onvoldoende aanvullende informatie aanlevert)

De afhandeling van de klachten heeft weer in goede samenwerking met de betreffende teams plaatsgevonden. Waar nodig hebben deze teams toegezegd de processen waarop terechte klachten betrekking hadden, aan te passen. In één geval: klacht camera Koemarkt, konden direct maatregelen getroffen worden om de klacht te ondervangen.

2. Zorgen/signalen medewerkers

Het aantal aan de FG in 2020 doorgegeven signalen van medewerkers is gedaald. Voor nu wijt ik dit aan het feit dat er in 2020 door de meeste medewerkers grotendeels thuis is gewerkt.

De signalen, voor zover (ook) relevant voor de gemeenteraad, betreffen de volgende onderwerpen:

- In lijn met de coronamaatregelen wordt overwogen hoorzittingen in het kader van bezwaarschriften in de openlucht plaats te laten vinden.
Opvolging signaal → Navraag leert dat er inderdaad hoorzittingen in de openlucht zijn gehouden. Strikt genomen is dat niet in strijd met de AVG, maar kan wel de privacy in de brede zin van het woord raken.
- Er blijven regelmatig op bureaus en in open kasten na werktijd gevoelige stukken liggen.
Opvolging signaal → door PIB wordt dit in diverse gremia aangekaart. Het is nog steeds een punt van aandacht.
- Gevraagd wordt om richtlijnen over hoe thuis – in coronatijd - papier te vernietigen.
Opvolging signaal → In augustus stelt de directie van Purmerend de Richtlijn vernietigen gegevensdragers vast waarin is opgenomen dat alle papier ter vernietiging wordt aangeboden in een afgesloten papiercontainer op één van de werklocaties.
- RAET (leverancier van Youforce) dreigt persoonsgegevens van medewerkers - waarover het beschikt als verwerker - voor eigen doeleinden te gebruiken.
Opvolging signaal → veelvuldig overleg - ook met RAET - over de handelwijze van RAET. Uiteindelijk zijn er geen concrete aanwijzingen dat RAET ook daadwerkelijk persoonsgegevens van medewerkers op deze manier ge-/misbruikt.
- Verbalen van BOA's zijn toegankelijk voor iedereen die toegang heeft tot de L-schijf map VTH.
Opvolging signaal → de BOA-documenten worden overgezet naar een alleen voor hen toegankelijke map op de L-schijf.
- Sollicitanten zijn verplicht de gemeentelijke privacyverklaring te accepteren als zij willen solliciteren; dit is in strijd met de AVG.

Opvolging signaal → RAET blijkt niet bereid dit verplichte veld op de website te verwijderen of om te zetten in een optioneel veld.

- Poststukken die te groot zijn voor de brievenbussen bij de achteringang blijven aan het eind van de middag regelmatig achter op de balie van Facilitair.
Opvolging signaal → er komt een aparte postkast waar ook grote stukken in passen.
- Medewerker stuurt mail met gevoelige persoonsgegevens naar het hele domein i.p.v. naar de collega voor wie de mail bedoeld is.
Opvolging signaal → in de privacywerkgroepen en rechtstreeks met betreffende medewerker besproken hoe mails die niet juist geadresseerd zijn bij de juiste collega terecht komen zonder datalekken te creëren.

3. DPIA's

Het jaarverslag over 2019 bevatte de volgende tekst:

“Samenvattend blijven DPIA's het volgende beeld opleveren:

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

In 2020 is de FG één DPIA voor advies aangeboden: de DPIA zaaksysteem. Op 6 april heb ik mijn advies op het concept uitgebracht. Eind december is deze DPIA nog niet vastgesteld, terwijl de implementatie van het zaaksysteem niet stil ligt. Hierdoor is onduidelijk in hoeverre met de adviezen van de FG respectievelijk de opmerkingen van de opsteller van de DPIA rekening wordt gehouden bij de implementatie.

Uit navraag blijkt dat gewerkt wordt aan meerdere DPIA's. Door het niet voltooien van deze DPIA's vóórdat nieuwe systemen worden aangeschaft, loopt de organisatie het gevaar dat met de systemen gepaard gaande risico's onvoldoende in beeld zijn.

- Datalekken

Het meldpunt datalekken heeft in 2020 geen datalekken behandeld die (ook) onder de verantwoordelijkheid van de gemeenteraad vielen.

NB De datalekken die onder de verantwoordelijkheid van het college en de burgemeester van Purmerend/Beemster vielen, kwamen in 2020 voor een groot deel voort uit slordigheidjes. Denk daarbij aan het verwisselen van bijlagen en het sturen van gegevens naar een verkeerd mailadres of oud postadres. Onduidelijk is of dit mede het gevolg is van de corona-situatie.

In Q4 van 2020 wordt de procesbeschrijving “Afhandelen melding datalek” geactualiseerd. De FG verlaat het meldpunt en de nieuwe ISO en privacyadviseur treden toe. Deze actualisering betekent niet dat de FG niet meer betrokken wordt bij datalekken:

- van ieder regulier afgehandeld datalek krijgt de FG achteraf een terugkoppeling;
- bij gevoelige datalekken wordt de FG in de gelegenheid gesteld te adviseren vóórdat een afhandelingsvoorstel aan de gemeentesecretaris respectievelijk de griffier wordt aangeboden.

Door deze nieuwe handelwijze is de FG in staat onafhankelijk te adviseren over datalekken.

In 2021 wordt gekeken hoe deze nieuwe handelwijze in de praktijk uitpakt.

1.3 Actielijst uit jaarverslag 2019, stand van zaken

Het jaarverslag 2019 bevatte de volgende actielijst. In de laatste kolom wordt aangegeven wat de stand van zaken t.a.v. deze acties is.

Permanente actiepunten

	Actiepunt	Toelichting	stavaza
1.	beoordelen actualiteit + bijhouden register van verwerkingsactiviteiten	het register is de basis voor inzicht in gegevensverwerkingen; actueel houden is prioriteit 1 Van gegevenseigenaren wordt verwacht dat zij hun verantwoordelijkheid hierin nemen	Zoals hierboven aangegeven, is door de privacyambassadeur van de griffie een eerste set gegevensverwerkingen aangeleverd. Het checken op nieuwe verwerkingen en op wijzigingen in bestaande verwerkingen moet een vast patroon worden.
2.	beoordelen rechtmatigheid gegevensverwerkingen		In 2020 niet opgepakt, in afwachting van de actie onder punt 1
3.	Monitoren aanwezigheid privacyconvenant bij gezamenlijk verwerkingsverantwoordelijken	De verplichting hiertoe is neergelegd in artikel 26 AVG	In 2020 zijn er geen nieuwe convenanten aangeleverd. Over dit onderwerp wordt gesproken door AP en VNG. Naar verwachting heeft de uitkomst van dit gesprek grote consequenties voor het kunnen zijn van gezamenlijk verwerkingsverantwoordelijken ¹
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 privacywerkgroepen	Presentaties hebben door de coronamaatregelen een groot deel van het jaar stil gelegen. In 2021 wordt dit weer opgepakt. De privacywerkgroepen hebben digitaal wel vergaderd Door de PO en de privacyadviseur wordt een begin gemaakt met het maandelijks plaatsen van een privacygerelateerd artikel op intranet
5.	monitoren vormgeven organisatorische privacy by design	met actiepunt 6 hieronder vormt dit punt de basis voor medewerkers om privacyproof te kunnen werken	Op een aantal punten zijn verbeteringen opgetreden; zie bv hierboven voor wat betreft de postbak.
6.	monitoren vormgeven privacy by design in systemen	dit punt wordt in samenwerking met de CISO (en waar mogelijk/nodig met externe organisaties) opgepakt	Één van de zaken die door de inwerkingtreding van de Wet politiegegevens (Wpg) van belang worden, is het scheiden van AVG-persoonsgegevens van

¹ hierover meer in het jaarverslag over 2021

	Actiepunt	Toelichting	stavaza
			Wpg-politiegegevens; dit moet in 2021 verder worden opgepakt Verbeteringen zijn bijv. opgetreden bij bovengenoemde camera's op de Koemarkt
7a.	monitoren uitvoeren DPIA's	Dit vindt plaats a.h.v. de verplichte DPIA-lijst van de AP	Met de eigenaar is periodiek overleg over de implementatie van het zaakstelsel
7b.	adviseren m.b.t. DPIA's	concept-DPIA's worden verplicht ter advisering aan de FG voorgelegd	Zie hierboven onder 1.2.2. onder 3.
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 CISO	Deze taak ligt nu bij de privacyadviseur. de FG blijft artikelen voor de PIB space schrijven
9.	afhandelen klachten betrokkenen	Betrokkenen kunnen zowel burgers als medewerkers zijn	Zie hierboven onder 1.2.2. onder 1.
10.	houden borgingsdocument-gesprekken de griffier	Dit vindt plaats a.h.v. bijgevoegd borgingsdocument	met de griffier heeft ook in 2020 weer een borgingsdocumentgesprek plaatsgevonden

Tijdelijke actiepunten

	Actiepunt	Toelichting	stavaza
1.	beoordelen rechtmatig toepassen grondslag toestemming	opgepakt in combinatie met structureel actiepunt 2	Zie permanente actie 2
2.	monitoren actualiseren procesbeschrijving afhandelen inzageverzoek	actualisatie vloeit voort uit nieuwe jurisprudentie	Door corona is het actualiseren nog niet opgepakt
3.	beoordelen aanwezigheid overige procesbeschrijvingen inzake rechten betrokkenen		er is een begin gemaakt met het beschrijven van de overige rechten betrokkenen
4.	Monitoren privacyaspecten Omgevingswet	Mede a.h.v. de DPIA 2019 DSO en Omgevingswet	In 2020 niet opgepakt
5.	(met Communicatie) verbeteren zichtbaarheid FG voor burgers en betrokkenen		Doorgeschoven naar 2021
6.	Monitoren effecten Reglement veilig gegevensgebruik en privacy	Monitoring zal plaatsvinden nadat de CISO en de PO alle teams hebben geïnformeerd over het Reglement	Door de coronamaatregelen hebben er zo goed als geen presentaties over het Reglement kunnen plaatsvinden

1.4 Wat viel verder op in 2020

1.4.1. Uit het borgingsdocumentgesprek

Net als in 2019, heeft de FG in Q4 met de griffier een borgingsdocumentgesprek gevoerd. Hieruit is het volgende vermeldenswaardig:

- Op basis van de Privacyshield-uitspraak (zie paragraaf 1.4.2) wordt de privacyverklaring op de (raads)website aangepast;
- Het lukt de privacyambassadeur ook in coronatijd om in de teamoverleggen terug te koppelen uit de privacywerkgroep-vergaderingen.

1.4.2. Overige onderwerpen

Van de onderwerpen die in het afgelopen jaar verder de revue zijn gepasseerd, wil ik de volgende aanstippen:

- Brexit en Privacyshield

Twee externe ontwikkelingen met hun weerslag op Beemster en Purmerendse gegevensverwerkingen.

Brexit:

In 2020 is een inventarisatie gedaan naar de verwerking van persoonsgegevens in het VK. Het aantal Britse verwerkers bleek heel beperkt en niet voor de raad actief te zijn. Daarnaast is de verwachting dat Brussel uiterlijk mei 2021 een adequaatheidsbesluit voor het VK goedkeurt. Wanneer dat er is, mogen persoonsgegevens zonder extra eisen met bedrijven in het VK uitgewisseld blijven worden.

Privacyshield:

In juli 2020 verklaart het Europese Hof van Justitie² dat uitwisseling van persoonsgegevens met Amerikaanse bedrijven niet langer zonder meer mogelijk is. De Amerikaanse veiligheidsdiensten blijken namelijk te allen tijde en zonder reden persoonsgegevens van Europeanen te (kunnen) vorderen.

Ook van Beemster persoonsgegevens is de kans reëel aanwezig dat die zich in de VS bevinden, bij grote bedrijven als Microsoft en Google, maar wellicht ook bij andere bedrijven³.

Nog steeds is onduidelijk hoe te handelen naar aanleiding van de uitspraak; de Europese privacytoezichthouders hebben nog geen sluitend antwoord. Aan het beter beveiligen van gegevens bij Microsoft wordt mede door het Rijk gewerkt. Voor verwerkingen bij andere Amerikaanse bedrijven wordt geadviseerd in kaart te brengen waar Beemster gegevens – waarschijnlijk - staan en op basis daarvan een risico-inschatting te maken óf en zo ja, welke maatregelen noodzakelijk/ gewenst zijn. De gemeentesecretaris van Purmerend heeft de opdracht gegeven die inventarisatie tot stand te brengen.

De FG heeft het college daarom geadviseerd om op basis van deze inventarisatie een risicogebaseerde en gemeentebrede afweging te maken t.a.v. te treffen maatregelen.

- Algoritmes en A(rtificial) I(ntelligence)

De Autoriteit Persoonsgegevens heeft dit onderwerp tot 2023 tot speerpunt van toezicht verklaard en Brussel is bezig met de voorbereiding van een AI-verordening. Uit:

- het onrechtmatig verklaren van de Systeem Risico Indicatie (SyRI) ter opsporing

² Schrems II-uitspraak

³ De inventarisatie is momenteel nog niet afgerond

van uitkeringsfraude⁴,

- de vraagtekens rondom het privacyproof zijn van het wetsvoorstel gegevensverwerking door samenwerkingsverbanden,
- de vragen van de minister van BZK inzake vermeend/onrechtmatig gebruik van de gezichtsherkenningsoftware van Clearview⁵ door gemeenten, blijkt dat dit extra toezicht en de verordening niet uit de lucht komen vallen.

Ook door Beemster en Purmerend worden algoritmes toegepast.

Gemeenten als Amsterdam publiceren op hun website inmiddels algoritmeregisters. Gemeenten als Enschede installeren een ethische commissie omdat wat technisch kán, niet altijd maatschappelijk en/of privacytechnisch wenselijk is.

De Algemene Rekenkamer heeft voor overheden een Toetsingskader algoritmes opgesteld.⁶

Op pagina 6 gaf ik aan dat ik periodiek overleg heb over algoritmes en AI.

Onderwerpen die in dit overleg ter sprake komen zijn bijvoorbeeld het systeem dat wellicht door Team Ondernijning wordt aangeschaft en draait op/met AI en diverse gemeentelijke prognosesystemen die gebruik maken van algoritmes.

De FG heeft het college verzocht maar verzoekt óók de raad om aandacht te hebben voor dit onderwerp; niet om de toekomst te willen tegenhouden, maar wel om te weten dat wát er door Beemster en Purmerend aan algoritmes en AI wordt aangeschaft– in ieder geval – op privacy-aspecten is getoetst.

- Verwerkers; aandachtspunten en (wan)gedrag

Verwerkers leveren een dienst aan verwerkingsverantwoordelijken zoals de raad en het college. Zij horen AVG-compliant te zijn en zich te gedragen overeenkomstig het gestelde in de verwerkersovereenkomst en eventuele aanvullende instructies.

Op pagina 7 heb ik een voorbeeld genoemd van hoe de praktijk kan afwijken van de theorie.

De FG onderkent het probleem om als kleine gemeente door een grote verwerker gehoord te worden, maar heeft het college evengoed verzocht al het mogelijke te doen om zo goed mogelijke overeenkomsten met deze verwerkers tot stand te brengen én om de naleving van deze overeenkomsten door de verwerkers te monitoren c.q. te (laten) auditen.

Ditzelfde verzoekt de FG ook aan de raad.

- Ondernijning

De aanpak van ondernijning staat momenteel in het centrum van de belangstelling. Maar wat is ondernijning? Een goede definitie bepaalt de omvang van de gegevens die in dat kader mogen worden verwerkt en bepaalt de spelers met wie gegevens mogen worden uitgewisseld. Om de gemeente hierbij te ondersteunen is vanuit het Rijk het “Privacyprotocol binnengemeentelijke gegevensuitwisseling ten behoeve van de bestrijding van ondernijning”⁷ uitgebracht.

De FG heeft het college verzocht zich bovenstaande vraag te stellen vóórdát Team Ondernijning in 2021 daadwerkelijk van start gaat en verzoekt het college zich deze vraag te blijven stellen iedere keer als een ander ondernijnings-onderwerp wordt opgepakt.

⁴ [ECLI:NL:RBDHA:2020:865, Rechtbank Den Haag, C-09-550982-HA ZA 18-388 \(rechtspraak.nl\)](#) NB Purmerend gebruikte dit systeem overigens niet

⁵ [De stand van gezichtsherkenning in Nederland \(volkskrant.nl\)](#) NB Purmerend gebruikt deze software overigens niet.

⁶ [Wat is het toetsingskader | Algoritmes | Algemene Rekenkamer](#)

⁷ [tk-bijlage-model-privacy-protocol-binnengemeentelijke-gegevensdeling.pdf](#)

- Kaderbrief
In april wordt de kaderbrief aan de raad (van Purmerend) aangeboden. Deze bevat weer diverse privacygerelateerde onderwerpen. Denk hierbij aan de aanschaf van een statisch-/dynamisch verkeersmodel, het uitlezen van camera's, het creëren van een lokaal team ondermijning en het aanpassen van werkplekken aan de AVG. In het kader van privacy by design is het goed als de FG en/of de PO tijdig bij deze ontwikkelingen kunnen aanhaken om niet achteraf te hoeven vertragen.

De FG heeft het college daarom gevraagd om de FG en/of de PO mee te laten lezen bij de concept-kaderbrief, zodat tijdig contact gezocht kan worden met de projectleiders van de diverse privacygerelateerde projecten.

- Privacygerelateerde effecten van corona
Zoals eerder aangegeven, ontsnapt niemand aan de effecten die (de) corona(maatregelen) heeft/hebben op het dagelijks werk.
De coronamaatregelen hebben echter ook zelf specifiek privacygerelateerde effecten. Hieronder vallen:
 - het privacyproof inregelen van camera's bij de begraafplaats waardoor nabestaanden, familie en vrienden toch in staat zijn om een begrafenis bij te wonen;
 - de plannen m.b.t. het aanbrengen van extra camera's rondom het stadhuis van Purmerend, mede om het gebrek van reguliere sociale controle te ondervangen;
 - de datalekken die ontstaan doordat de weinige medewerkers die aanwezig zijn, op een voor iedereen zichtbare plek (bv op de hoek van een bureau) stukken achterlaten die andere collega's op een later tijdstip kunnen meenemen. Hiervoor wordt door PIB aandacht gevraagd, maar het is een terugkerend punt.

Deel 2 Vooruitblik naar 2021; fusiejaar

2.1 Privacyproof fuseren tijdens een pandemie

Privacy tijdens het fusieproces de plaats geven die nodig is en tegelijkertijd de reguliere processen – zo privacyproof mogelijk - doorgang laten vinden is een grote uitdaging.

2021 kent echter meer uitdagingen en actiepunten dan de fusie.

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 De griffier is hiervoor het eerste aanspreekpunt	Permanente actie
2.	beoordelen rechtmatigheid gegevensverwerkingen	De actie wordt opgepakt a.h.v. de door de griffie doorgegeven data	“
3.	Monitoren aanwezigheid privacyconvenant bij gezamenlijk verwerkingsverantwoordelijken	De verplichting hiertoe is neergelegd in artikel 26 AVG NB de uitspraak van de VNG/AP van maart 2021 dat organisaties met een wettelijk mandaat geen gezamenlijk verwerkingsverantwoordelijke met een gemeentelijk bestuursorgaan kunnen zijn, beïnvloedt dit actiepunt	
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 kunnen 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	“
7.	adviseren m.b.t. (uitvoering) DPIA's	concept-DPIA's worden verplicht ter advisering aan de FG voorgelegd	“
8.	afhandelen klachten betrokkenen	Betrokkenen kunnen zowel burgers als medewerkers zijn	“
9.	voeren borgingsdocument-gesprek met de griffier	Dit vindt plaats a.h.v. het borgingsdocument (dat door de VNG in 2021 geactualiseerd is)	“

2.2.2. Tijdelijke actiepunten

	Actiepunt	Toelichting	Planning
1.	Monitoren privacyaspecten Omgevingswet	Mede a.h.v. de DPIA 2019 DSO en Omgevingswet	Vanaf Q2
2.	Monitoren nieuwe afspraken Meldpunt datalekken	Nagaan of de FG conform de gewijzigde procesbeschrijving bij de afhandeling van datalekken betrokken wordt	Vanaf Q2

	Actiepunt	Toelichting	Planning
3.	(met Communicatie) verbeteren zichtbaarheid FG voor burgers en betrokkenen		Vanaf Q3
4.	Monitoren effecten Reglement veilig gegevensgebruik en privacy	Monitoring zal plaatsvinden nadat de CISO en de PO alle teams hebben geïnformeerd over het Reglement	Vanaf Q3