GEMEENTE BEEMSTER
WERELDERFGOED

MEMO

Aan	:	De raadsfracties
Van	:	A.J.M. van Beek, burgemeester
Datum	:	21 maart 2017
Onderwerp	:	**beantwoording openstaande technische vragen van de VVD over de bewerkersovereenkomsten met Purmerend, informatiebeveiliging, privacy en integriteit** (commissie 28 februari 2017)
Bijlagen	:	2

Bij de technische vragen voor de commissievergadering van 28 februari 2017 heeft de fractie van de VVD nadere vragen gesteld naar aanleiding van de thema-avond 24 januari 2017 inzake informatie beveiliging en de bewerkersovereenkomsten die als bijlage zijn gevoegd bij de antwoorden op de eerdere technische vragen hierover (commissie 7 februari 2017).
In deze memo treft u de antwoorden op deze nadere vragen aan.

Vraag 1
Thema avond 24 januari 2017 inzake informatie beveiliging en de door u getekende bewerkersovereenkomsten als bijlage bij de technische antwoorden van commissie van 7 februari 2017:
De toegezonden overeenkomsten zijn getekend op 24 sept. 2013, 20 dec. 2013 en de laatste op 7 jan. 2014. De data echter is eerder overgegaan namelijk op 1 jan. 2013. Kunnen wij nog claims verwachten over die voorliggende maanden? Een recent voorbeeld is YAHOO met een claim voor een datalek van jaren terug. Hoe groot is het risico op een claim en hoe onderbouwt u die?

Antwoord 1
Op 1 januari 2013 zijn Beemster en Purmerend een samenwerking aangegaan op het terrein sociaal domein en het terrein OOV. Pas op 1 januari 2014 is de overall samenwerking van start gegaan. De bewerkersovereenkomst m.b.t. de data die samenhangen met de overall samenwerking, is dus tijdig aangegaan. Het is juist dat de bewerkersovereenkomst m.b.t. de data die samenhangen met de partiële samenwerking te laat is afgesloten.
Gezien het feit dat de overdracht van data t.b.v. de partiële samenwerking plaatsvond binnen de sfeer van 2 gemeentelijke overheden, is de kans op claims niet uitgesloten, maar is deze kans kleiner dan wanneer de data zouden zijn overgedragen naar bv een particulier bedrijf buiten de EU.
Vervolgens is het de vraag of een claim – gezien het bepaalde in artikel 49 Wbp – kans van slagen heeft. Een betrokkene moet dan al bewijzen dat hij schade heeft geleden omdat de verwerking van zijn data door de gemeente Purmerend (ten behoeve van de gemeente Beemster) heeft plaatsgevonden zonder bewerkersovereenkomst.
Voor de goede orde kan hier nog aan worden toegevoegd dat op het niet (tijdig) afsluiten van een bewerkersovereenkomst op dit moment nog geen boete staat. Dit wordt pas bij de inwerkingtreding van de AVG op 25 mei 2018 anders; dan staat op het niet (tijdig) afsluiten van een bewerkersovereenkomst een boete van maximaal 10 miljoen euro.

Vraag 2
Art 3.3 Hoe is dit geborgd en wie doet op welk moment een audit?

Antwoord 2
Het Gemeentelijk informatiebeveiligingsbeleid van Purmerend 2015 is uitgewerkt in een Uitvoeringsplan Gemeentelijk Informatiebeveiligingsbeleid 2015.
Halfjaarlijks wordt aan de raden van Purmerend en Beemster een verslag informatieveiligheid en privacy aangeboden.
Er worden verschillende audits en assessments uitgevoerd:

- Zelfevaluatie Basisregistratie Personen. Het resultaat is “goed” conform de geldende normen. Ten aanzien van de gemeente Beemster stond er nog wel een actie open om documenten die te vroeg zijn overgedragen aan het Waterlands Archief terug te halen. Deze actie is inmiddels uitgevoerd; de stukken liggen in de Beemster(kluis).
- Zelfevaluatie Paspoorten en Nationale Identiteitskaarten. Het resultaat is “goed” conform de geldende normen.
- SUWINET: in het eerste halfjaar bleek dat onze organisatie niet volledig voldeed aan de gestelde normen. Hierop zijn maatregelen ter verbetering genomen en 20 oktober kwam het bericht binnen van het ministerie van Sociale Zaken en Werkgelegenheid dat daar wel aan wordt voldaan.
- DigiD audit 2016: in het najaar zijn twee nieuwe DigiD-aansluitingen in gebruik genomen in verband met de afhandeling van bezwaren belastingen en heffingen bij het bedrijf GouwIT. Binnen twee maanden na ingebruikname moet een assessment zijn doorlopen. Vlak voor kerst is dit afgerond en is het positieve rapport van de auditor ingediend bij Logius In het begin van 2017 wordt het assessment van de twee oudere DigiD-aansluitingen bij een andere leverancier afgerond. Deze audit is uitgevoerd door een auditor die is ingeschreven in het NOREA-register. Zie: https://www.norea.nl/

In 2016 is er geen verplichting geweest tot het uitvoeren van een BAG-audit.
Momenteel voert de accountant als onderdeel van de controle op jaarrekening een IT-audit uit. Daarnaast laat Purmerend op vrijwillige basis penetratietests uitvoeren door een gespecialiseerd bedrijf.

Vraag 3
Art 3.5 geheimhouding door medewerkers. Hebben betreffende medewerkers daar apart voor getekend naast de reguliere clausules inzake verantwoordelijk en aansprakelijkheid in hun arbeidsovereenkomst c.q. aanstelling? Worden daar ook sancties bij genoemd in geval van overtreding?

Antwoord 3
Artikel 2:5, eerste lid van de Algemene wet bestuursrecht bepaalt het volgende:

Een ieder die is betrokken bij de uitvoering van de taak van een bestuursorgaan en daarbij de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, en voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van die gegevens, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht of uit zijn taak de noodzaak tot mededeling voortvloeit.

Schending van deze algemene geheimhoudingsplicht levert een misdrijf op o.g.v. artikel 272 Wetboek van strafrecht:

Artikel 272 *1 Hij die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie*.

(= max. € 20.500,-)

Voor medewerkers met een dienstverband vormt deze bepaling een aanvulling op de af te leggen eed; zie bijlage. Daarnaast wordt van medewerkers geen expliciete geheimhoudingsverklaring gevraagd.
NB ingehuurd personeel/externen leggen in aanvulling op artikel 2:5 Awb een aparte integriteits- en geheimhoudingsverklaring af; zie bijlage.

Vraag 4
Art 3.8 controle/audit/oordeel. Op de thema avond werd op onze vraag of deze afdeling in Purmerend, ISO gecertificeerd is, ontkennend geantwoord. In de stukken staat “Purmerend overlegt een schriftelijk oordeel van een accountant als Beemster er om vraagt.” Is dit al gebeurd en indien ja, wat was de uitkomst van die controle/audit/oordeel.

Antwoord 4
Gemeente Purmerend hanteert (net als andere gemeenten in Nederland) de Baseline Informatiebeveiliging Gemeenten als normenkader. De BIG is gebaseerd op de NEN/ISO 27002:2007.
Er is door Beemster geen oordeel van een accountant of gelijkwaardige deskundige gevraagd aan Purmerend.
Medio dit jaar start de Eenduidige Normatiek Single Information Audit ter vervanging van de afzonderlijke audits (BRP, BAG, DigiD en Suwinet). Elke gemeente moet daaraan meedoen. Externe auditors beoordelen dit self-assessment waarna (voor medio 2018) de colleges verantwoording moeten afleggen aan hun raden.