raadsmededeling

zaak/onderwerp	Z-16-13934 / Openbaarheid privacy gevoelige gegevens maart 2016
portefeuillehouder	M.A. den Boer
team	Bedrijfsondersteuning
opgesteld door	R.J.M. van der Zande
datum/nr	17 maart 2016 / CB-16-1606

Geachte raad,

Op 9 maart 2016 hebben wij u per raadsmededeling geïnformeerd over de melding die wij op 25 februari 2016 hebben gekregen van de Informatiebeveiligingsdienst (IBD), dat bestanden met privacygevoelige informatie tijdelijk openbaar toegankelijk zijn geweest. Het betrof hier onder andere adresgegevens en Burgerservicenummers (BSN) van inwoners van de gemeente Oegstgeest. Met deze mededeling willen wij een aantal zaken nader toelichten die in uw raad op 10 maart 2016 aan de orde zijn geweest.

Wij benadrukken hierbij dat wij het betreuren dat deze gegevens van inwoners tijdelijk openbaar toegankelijk zijn geweest via het internet. Er is sprake van een menselijke fout waarbij de geldende regels en protocollen voor het gebruik van privacy gevoelige informatie overtreden zijn. Wij doen ons uiterste best om de inwoners die dit betreft te informeren en te helpen waar dit noodzakelijk is.

We lichten in deze raadsmededeling toe wat er precies is gebeurd, om welke persoonsgegevens het gaat en hoe deze gegevens benaderbaar zijn geweest, voor zover nu bekend is. Daarnaast informeren wij u over het tijdspad, informatie aan betrokken inwoners, aansprakelijkheid en informatieveiligheid.

Een technisch onderzoek in opdracht van de gemeente Rotterdam om te onderzoeken hoe en of de gegevens van Rotterdam en Oegstgeest zijn benaderd is nu nog gaande. Wanneer dit onderzoek is afgerond, zullen wij u hier uiteraard nader over informeren. Het gespecialiseerde onderzoeksbureau heeft als voorlopige conclusies op 7 maart laten weten niet volledig uit te kunnen sluiten dat er géén gebruik is gemaakt van de mogelijkheid om de betreffende bestanden te benaderen. Wel gaf het bedrijf aan de kans zeer klein te achten. Op basis van die informatie zijn wij de betrokken inwoners en u gaan informeren.

Wat is er precies gebeurd?
Een oud-medewerker van een ICT-bedrijf dat in opdracht van de gemeente Oegstgeest werkte heeft in de periode 2007-2009 gemeentelijke belastingbestanden met daarin persoonsgegevens op zijn privéapparatuur opgeslagen. Hoewel dit in die periode niet ongebruikelijk was, is het niet toegestaan om deze werkbestanden ook op te slaan. Er is verzuimd deze werkbestanden te verwijderen en deze zijn vervolgens (onbewust) op een externe (Back up) harde schijf opgeslagen. De betreffende externe harde schijf is door de medewerker ook gebruikt voor privé opslag van foto's, films etc. en bij het mogelijk maken van het bekijken van deze foto's is de beveiliging naar internet (tijdelijk) onderbroken geweest. De oud-werknemer heeft daarbij de interne regels van het ICT-bedrijf overtreden.

De oud-werknemer van het ICT-bedrijf was in de periode 2001-2004 in dienst van de gemeente Rotterdam en is in 2008 weer in dienst getreden van de gemeente Rotterdam. Vandaar dat in het bestand van de oud-medewerker ook werkdocumenten stonden van de gemeente Rotterdam. Vanaf het moment van de ontdekking van de link tussen Oegstgeest en Rotterdam, is er ambtelijk en bestuurlijk overleg geweest tussen beide gemeenten.

Welke gegevens waren tijdelijk benaderbaar?
Gegevens vanuit de applicatie voor de gemeentelijke belastingen. Deze gegevens betreffen onder meer naam, geboortedatum, adresgegevens, geslacht en BSN-nummer. Het gaat om gegevens uit de jaren 2007, 2008 en 2009.

Naast persoonlijke gegevens stonden er ook gemeentelijke belastinggegevens OZB van deze bewoners in de bestanden. Deze gegevens zijn echter openbaar, dus voor iedereen opvraagbaar. Het betreft hier WOZ-waarde, taxatiewaarde en huurwaarde.

In de bestanden stonden geen bankrekeninggegevens.

Hoe eenvoudig was het om de gegevens te benaderen?
In tegenstelling tot de berichtgeving en uitspraken hebben de BSN en NAW-gegevens niet "op straat gelegen". Wel is het mogelijk geweest om de gegevens te vinden, wanneer daar gericht naar gezocht werd. Wij hebben de IBD verzocht om een reactie op dit punt naar aanleiding van hun melding. Deze melding is afkomstig van een andere gemeente. De IBD doet echter geen uitspraken over hun zoekmethodes en hoe de melding bij de IBD zelf terecht is gekomen. Wel geven zij de volgende verklaring af:

"De IBD heeft de set van gegevens van Oegstgeest aangetroffen bij een uitgebreid onderzoek naar aanleiding van een andere melding. Deze bewuste melding had geen betrekking op persoonsgegevens, maar betrof wel gemeentelijke informatie. De IBD doet i.v.m. de aard van hun werkzaamheden geen mededelingen over individuele meldingen noch over de middelen die tot haar beschikking staan bij een onderzoek. Het is volgens de experts van Rotterdam hoogst onwaarschijnlijk dat de gegevens benaderbaar zijn geweest zonder een zeer gerichte en specialistische zoekactie. Het zoeken naar een BSN-nummer zou hierbij niet voldoende zijn geweest."

Dit laatste wordt bevestigd door de onderzoekers van het gespecialiseerde bedrijf dat de gemeente Rotterdam opdracht heeft gegeven het technisch onderzoek laten doen. In dat onderzoek worden mede de gegevens van de gemeente Oegstgeest geanalyseerd. Er zijn ook geen sporen van gerichte zoekacties naar deze gegevens op internet aangetroffen. Daarnaast geven diverse gespecialiseerde instanties aan dat adresgegevens en BSN gegevens weliswaar gebruikt kunnen worden om identiteitsfraude te plegen, maar dat hier meerdere gecombineerde acties voor nodig zijn en samenwerking met malafide partijen.

Hoe lang zijn de gegevens benaderbaar geweest?
Uit de voorlopige verklaring van de betreffende medewerker van de gemeente Rotterdam blijkt dat het openbaar toegankelijk zijn van de oude werkbestanden kan hebben plaatsgevonden in de periode begin januari tot eind februari 2016. Het technisch onderzoek zal uitwijzen of dit ook zo is. Hoewel onwaarschijnlijk kunnen we dus niet uitsluiten dat de gegevens zijn benaderd, vandaar de melding.

Tijdlijn
Met onderstaande tijdlijn schetsen wij voor uw raad het verloop van de gebeurtenissen en de werkzaamheden gedurende de afgelopen periode:

De melding & eerste acties: *donderdag 25 en vrijdag 26 februari*

Donderdag 25 februari zijn wij geïnformeerd door het ICT-bedrijf, naar aanleiding van de melding door de informatiebeveiligingsdienst van de VNG (IBD) dat het mogelijk was om gegevens die privacygevoelig waren te benaderen. De medewerker van Rotterdam heeft er vervolgens onmiddellijk voor gezorgd dat zijn apparatuur niet langer toegankelijk was. De IBD heeft dit ook direct getest en bevestigd. Na de melding heeft de Rotterdamse medewerker meteen inzicht gegeven in de bestanden, om zo te kunnen bepalen wat voor gegevens mogelijk toegankelijk zijn geweest. Toen bleek dat niet alleen bestanden van de gemeente Rotterdam opvraagbaar zijn geweest, maar ook van de gemeente Oegstgeest, heeft de gemeente Rotterdam meteen ambtelijk contact gelegd tussen beide gemeenten. De gemeente Rotterdam heeft verder aangegeven dat de medewerker direct al zijn privé-apparatuur voor nader onderzoek heeft ingeleverd en alle data veilig gesteld voor analyse.

Stand van zaken tot en met maandag 14 maart 2016
Aantal telefoontjes tot en met maandag:

Dag	9/3	10/3	11/3	14/3	Totaal
Aantal	91	63	21	7	182

Aantal terugbelnotities: 15
Aantal ontvangen klachten: 2
Aantal voorlopige aansprakelijkheidsstellingen: 9

De meeste reacties tot nu toe gaan over de zorg van betrokkenen dat er wellicht iets met hun persoonsgegevens kan gebeuren. Ook zijn mensen – terecht – boos over dit incident en willen dit melden. Het algemene beeld is dat men zich gehoord en goed geholpen voelt.

Vooralsnog sturen wij geen extra brief naar de betrokkenen of organiseren wij een informatieavond. Wij hebben geen nieuwe informatie voor de inwoners en wij hebben vanuit de medewerkers van het callcenter ook geen signalen gekregen dat de aangeboden informatie onvoldoende is. Mochten wij nieuwe relevante informatie hebben dan zullen wij die uiteraard met betrokkenen delen via een brief of informatieavond.

De ontvangen klachten en voorlopige aansprakelijkheidsstellingen worden conform ons beleid behandeld.

Aansprakelijkheid
Als inwoners die in de bestanden voorkomen, een vermoeden van misbruik van hun persoonsgegevens (voor zover het BSN, NAW betreft) hebben en daadwerkelijk schade hebben geleden, kijkt de gemeente Oegstgeest uiteraard of de geleden schade te herleiden is naar dit incident. Elke casus is anders en maatwerk en extra aandacht zijn hierbij geboden. Om vast te stellen of er een relatie is met de data van de gemeente Oegstgeest dient te worden benadrukt dat er altijd eerst sprake moet zijn van schade door misbruik van BSN en NAW (dit zijn de gegevens die in de database stonden waarmee misbruik mogelijk is). Daarvoor zal ook overleg zijn met het Meldpunt Identiteitsfraude. Daarna gaan wij in gesprek om samen met de desbetreffende persoon te bezien wat er aan de hand is.

De gemeente zelf gaat haar ICT-leverancier aansprakelijk stellen voor de schade die zij door deze situatie oploopt.

Bestuurlijke boete
De Autoriteit Persoonsgegevens kan bij overtreding van de meldplicht datalekken uit de Wet bescherming persoonsgegevens een bestuurlijke boete opleggen. Deze bestuurlijke boete bedraagt ten hoogste het bedrag van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht. Dat is per 1 januari 2016 maximaal 820.000 euro.
In de Boetebeleidsregels Autoriteit Persoonsgegevens 2016 staat hoe de Autoriteit Persoonsgegevens de hoogte van boetes bepaald.

Bindende aanwijzing
Is de overtreding niet opzettelijk gepleegd? En is er geen sprake van ernstig verwijtbare nalatigheid? Dan legt de Autoriteit Persoonsgegevens eerst een bindende aanwijzing op. Daarna legt de Autoriteit Persoonsgegevens eventueel een bestuurlijke boete op.

Overwegingen boete datalek
Bij het opleggen van een bestuurlijke boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden van het geval. Een omstandigheid van het geval is bijvoorbeeld dat de gelekte gegevens niet door derden zijn ingezien.

Wij hebben tot op heden gehandeld binnen de regelgeving voor het melden van datalekken en wachten de procedure die de Autoriteit gaat voeren af.

Op vrijdag 26 februari zijn de benodigde gegevens verzameld om het datalek te kunnen melden bij de Autoriteit Persoonsgegevens. Deze eerste melding is op vrijdagochtend 26 februari gedaan.

Maandag 29 februari tot maandag 7 maart

Op maandag 29 februari is definitief vastgesteld dat het voor Oegstgeest gaat om bestanden, benodigd voor zogenaamde WOZ taxaties, met privacy gevoelige gegevens. Voor Rotterdam betrof het belastinggegevens met privacy gevoelige gegevens over de periode 1996-2004. Vanwege de eigenstandige verantwoordelijkheden van gemeenten als beheerder van de Basisregistratie Persoonsgegevens (BRP) is vervolgens afgesproken dat in nauwe afstemming met Rotterdam wij onze eigen communicatie naar de inwoners zou verzorgen.

Voor de communicatie naar Oegstgeester betrokkenen was het noodzakelijk om meer te weten te komen over de aard en de omvang van het lek. Er is door de gemeente Rotterdam aan een gespecialiseerd bedrijf opdracht verstrekt om hier technisch onderzoek naar te doen. Gelijktijdig is er uitbreiding van de capaciteit van ons Telefonisch Informatie Punt (14071) georganiseerd door een tijdelijk callcenter in te richten, werd er gewerkt aan een bewonersbrief, raadsmededeling en is een Q&A-document opgesteld voor medewerkers van het tijdelijke callcenter en voor op de gemeentelijke website zodat betrokkenen ook online meer informatie over het voorval konden opzoeken.

Verder zijn de werkbestanden geanalyseerd met behulp van de oude belastingsystemen. Daarnaast is een vergelijking gemaakt met de BRP om uit het totale bestand te kunnen bepalen welke inwoners een brief zouden moeten krijgen omdat ze mogelijk getroffen werden. Uit de analyse blijkt dat in de bestanden 9.267 personen worden genoemd. Van deze personen is nagegaan of zij nog woonachtig zijn in Oegstgeest en nog in leven zijn. Uit deze vergelijking is gebleken dat: inmiddels 1.110 zijn overleden, 6.542 personen nog in de gemeente Oegstgeest wonen, 252 personen zijn geëmigreerd en 1.363 personen wonen elders in Nederland. De mensen die nog in Oegstgeest wonen of elders in Nederland (6.542 en 1.363 personen) hebben een brief gehad. In totaal hebben dus circa 7.900 personen een brief gekregen. De andere categorieën volgens de wettelijke bepalingen niet.

Maandag 7 maart tot maandag 14 maart

Maandag 7 maart liet het gespecialiseerde bedrijf ons weten niet volledig uit te kunnen sluiten dat er géén gebruik is gemaakt van de mogelijkheid om de betreffende bestanden te benaderen. Wel gaf het bedrijf aan de kans zeer klein te achten. Deze informatie was voor ons voldoende om de brief aan betrokkenen en de brief ter informatie aan uw raad af te kunnen ronden. Die dag is de brief aan betrokkenen gedrukt (in totaal dus 7.900) en voor verzending op dinsdag 8 maart aangeboden aan TNT Post. Na vaststelling in het college is de raadsmededeling aan uw raad woensdagochtend 9 maart aangeboden met een kopie van de brief aan betrokkenen. Diezelfde dag zijn de brieven bij de betrokkenen bezorgd.

Op dinsdag 8 maart is bij de Autoriteit Persoonsgegevens de bestaande melding geactualiseerd en definitief gemaakt.

Op basis van de reacties die wij via het speciale telefoonnummer, het backoffice team en social media binnenkrijgen vanaf woensdag 9 maart, zijn de Q&A's voortdurend aangepast en aangevuld. Daarnaast werkten wij met terugbelnotities in bijzondere situaties.

Hulp aan betrokkenen

Om de inwoners die een brief hebben ontvangen te kunnen ondersteunen is er vanaf woensdag 9 maart via een apart in de brief genoemd nummer (1e-lijns hulp) een tijdelijk callcenter ingericht met 10 telefoonlijnen. Daarnaast is er een 2e-lijns team ingericht die complexere vraagstukken kan behandelen en terugbelnotities kan uitvoeren. Het 2e-lijns team behandelt ook klachten. Daarnaast is er zoals gezegd een speciale Q&A aanwezig op www.oegstgeest.nl met veel gestelde vragen en antwoorden.

Informatiebeveiliging
De gemeente heeft een Statuut Informatiebeveiliging, vastgesteld door het College in oktober 2013. Dit statuut is regionaal ontwikkeld in samenwerking met Servicepunt71 (SP71).

In 2015 is gestart om in samenwerking te komen tot een regionaal gedragen informatiebeveiligingsbeleid dat gebaseerd is op Baseline Informatieveiligheid Nederlandse Gemeenten (BIG) waarmee is ingestemd tijdens de Buitengewone Algemene Leden Vergadering (BALV) van de VNG in november 2013. Dit beleid zal het huidige Statuut gaan vervangen in het tweede kwartaal 2016.

Vooruitlopend op dit beleid is Oegstgeest lokaal aan de slag om het huidige Statuut aan te vullen met een vastgelegde governance op het gebied van Informatieveiligheid. Het voorstel om dit formeel vast te leggen is voor 29 maart geagendeerd voor het College. De raad zal hierover, na behandeling in het College worden geïnformeerd.

In de aanpak vanaf de melding op 25 februari tot op heden hebben wij in lijn met het genoemde governance Informatieveiligheid gehandeld.

Mocht u na het lezen van deze brief nog aanvullende vragen hebben over het incident waarbij persoonsgegevens toegankelijk zijn geweest of over het beleid dat wij hebben om dit soort incidenten te voorkomen, dan zijn wij natuurlijk graag bereid deze te beantwoorden. Afhankelijk van de stand van zaken zullen wij u uiterlijk 31 maart opnieuw schriftelijk en/of mondeling informeren.

Burgemeester en wethouders van Oegstgeest

de secretaris
H.A. Leegstra

de burgemeester
E.R. Jaensch