Intern onderzoek naar het op 25 februari 2016 gemelde datalek in de gemeente Oegstgeest

Oegstgeest, 29 juni 2016
Directie Bestuur- en Concernondersteuning
Gemeente Oegstgeest

Aanleiding en aanpak intern onderzoek

Op 25 februari 2016 ontving de gemeente Oegstgeest melding dat bestanden met daarin privacygevoelige gegevens van een deel van de inwoners en oud-inwoners tijdelijk openbaar zijn geweest via internet. Deze melding werd gedaan door de leverancier.
Vanaf 1 januari 2016 is de meldplicht datalekken – in aanvulling op de Wet bescherming persoonsgegevens – in werking getreden. De gemeente Oegstgeest heeft het datalek ruim binnen de daarvoor gestelde termijn aan de Autoriteit Persoonsgegevens (AP) gemeld.

Voor een overzicht van wat er daarna is gebeurd, wordt in dit intern onderzoek verwezen naar de raadsmededeling d.d. 17 maart 2016 met als onderwerp 'Openbaarheid privacy gevoelige gegevens maart 2016'.

Interne evaluatie
Er heeft inmiddels een interne evaluatie (bijlage 1) plaatsgevonden waarin de volgende vraag centraal stond:
'In hoeverre is de *aanpak* adequaat (tijdig en zorgvuldig) geweest en voldoet het 'proces melden datalek en beveiligingsincident' op basis van de opgedane ervaringen?'

Doel- en vraagstelling intern onderzoek
Doel van dit intern onderzoek is beantwoording van de vraag hoe dit datalek heeft kunnen ontstaan en hoe we kunnen voorkomen dat zich een vergelijkbaar incident nog eens voordoet.

Achtereenvolgens worden de volgende vragen beantwoord:
1. Hoe was de beveiligingssituatie en de aanpak van de gemeente Oegstgeest in de tijd dat de oud-leverancier werkzaamheden voor de gemeente verrichte?
2. Is de gemeente zorgvuldig te werk gegaan in de gemaakte afspraken met de oud-leverancier?
3. Wat is de status van de informatieveiligheid van de gemeente?
4. In hoeverre zijn de al ingezette verbeteringen voldoende om herhaling te voorkomen?
5. Welke acties zijn aanvullend nodig om het herhalingsrisico tot een minimum te beperken?

Dit onderzoek heeft betrekking op het datalek dat op 25 februari 2016 werd geconstateerd. In de laatste paragraaf worden ook de acties geschetst die in bredere zin worden ondernomen ten behoeve van informatiebeveiliging in Oegstgeest.

Hoe was de beveiligingssituatie en de aanpak van de gemeente Oegstgeest in de tijd dat de oud-leverancier werkzaamheden voor de gemeente verrichte?

Dit datalek vindt zijn oorsprong in de jaren 2007-2009, toen de oud-leverancier diensten verleende aan de gemeente Oegstgeest. In die tijd was het in de gemeente Oegstgeest (en ook in andere gemeenten) gebruikelijk dat externen met eigen apparatuur werkte en met behulp daarvan diensten verrichte voor de gemeente.

Ten tijde van het ontstaan van dit datalek was het vigerende informatiebeveiligingsbeleid van de gemeente Oegstgeest (uit februari 2005) van toepassing. De term 'informatiebeveiliging' wordt in dit beleid als volgt gedefinieerd:

> De gemeente Oegstgeest hanteert de volgende definitie van het begrip **Informatie-beveiliging:**
>
> *Het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de beschikbaarheid, integriteit en exclusiviteit van een informatiesysteem en de daarmee gerelateerde informatie (data).*

In dit beleid worden drie beveiligingsaspecten genoemd, waaronder exclusiviteit. Dit houdt in:

> In lijn met de 'Code voor Informatiebeveiliging' (2) gaat de gemeente Oegstgeest daarbij uit van de volgende drie beveiligingsaspecten, die tezamen de betrouwbaarheid bepalen:
>
> - **Beschikbaarheid:** *de mate waarin een informatiesysteem in bedrijf is op het moment dat de organisatie het nodig heeft;*
> - **Integriteit:** *de mate waarin het informatiesysteem zonder fouten is;*
> - **Exclusiviteit (vertrouwelijkheid):** *de mate waarin de toegang tot en de kennisname van een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep gerechtigden.*

Hoewel niet specifiek ingegaan wordt op het opslaan van gegevens op apparatuur die niet in eigendom is van de gemeente Oegstgeest, is één van de doelstellingen van het informatiebeveiligingsbeleid 'een betrouwbare gegevensverwerking te waarborgen'.

> Gezien het belang van betrouwbare gegevensverwerking en de noodzaak om hier controle over uit te oefenen en verantwoording daarover af te leggen heeft gemeente Oegstgeest een organisatiestructuur en processen ingericht voor informatiebeveiliging. Informatiebeveiliging zorgt ervoor dat adequate maatregelen worden gedefinieerd die een betrouwbare gegevensverwerking waarborgen, dat de maatregelen worden geïmplementeerd en dat de naleving wordt gecontroleerd.

In het informatiebeveiligingsbeleid wordt ook aandacht besteed aan afspraken over informatiebeveiliging met externe partijen. Die moeten schriftelijk worden vastgelegd, zo schrijft het beleid voor. Ook sancties ten aanzien van externe partijen moeten schriftelijk worden vastgelegd in de overeenkomsten met deze partijen.

> 7. Afspraken over informatiebeveiliging tussen interne en externe partijen worden schriftelijk vastgelegd.
>
> *Toelichting:*
> Afspraken met bedrijven over de behandeling van informatie worden in overeenkomsten vastgelegd. Speciale aandacht is vereist voor free-lance en van derden ingehuurd personeel.

Is de gemeente zorgvuldig te werk gegaan in de gemaakte afspraken met de oud-leverancier?
In het contract met de oud-leverancier wordt ingegaan op de wijze waarop de leverancier omgaat met gegevens van de gemeente Oegstgeest. De leverancier verbindt zich daarin onder andere aan het volgende:

- De leverancier erkent dat de informatie die aan haar bekend wordt in het kader van de uitvoering van werkzaamheden een strikt vertrouwelijk karakter dragen;
- De leverancier zal op geen enkele wijze het bestaan, de inhoud van de relatie met de gemeente, alsmede de informatie welke aan haar bekend wordt aan derden bekend maken, anders dan na voorafgaande schriftelijke toestemming van de gemeente. Deze verplichting geldt zowel tijdens de looptijd van de overeenkomst als na afloop daarvan;
- Redelijke maatregelen in acht te nemen voor een veilige berging of opslag van de gegevens;
- De gegevens niet langer onder zijn berusting te houden dan voor het uitvoeren van de overeengekomen verplichtingen en de gegevens na volledige nakoming van de verplichtingen weer ter beschikking te stellen van de gemeente dan wel te vernietigen;
- De overeengekomen verplichtingen uitsluitend te laten uitvoeren door personen waarvan de leverancier in redelijkheid meent dat zij betrouwbaar zijn;
- Medewerking te verlenen aan het uitoefenen van toezicht door of namens de gemeente op bewaring en gebruik van gegevens;
- De leverancier zal zich maximaal inspannen ervoor te zorgen dat haar personeelsleden en/of voor haar werkzame derden op de hoogte zijn van de verplichtingen en deze stipt zullen naleveren. De leverancier draagt er zorg voor dat de bij de werkzaamheden betrokken werknemers en derden contractueel tot geheimhouding zijn verplicht.

Wat is de status van de informatieveiligheid van de gemeente?

Met informatieveiligheid bedoelen we in dit onderzoek het beleid dat gaat over informatieveiligheid in algemene zin, niet specifiek over de GBA. Voor de GBA geldt aparte regelgeving waar Oegstgeest al jaren aan voldoet met hoge tot zeer hoge scores.

Het laatste lokale informatieveiligheidsbeleid en -plan van Oegstgeest dateert uit 2005. In de periode tussen 2005 en 2013 is er geen nieuw beleid ontwikkeld en beperkte inzet geweest t.a.v. informatieveiligheid. In 2013 is in regionaal verband een gezamenlijk "Statuut informatiebeveiliging Gemeente Leiden, Leiderdorp, Oegstgeest, Zoeterwoude & Servicepunt71" opgesteld. Met de komst van een nieuwe Senior Adviseur Informatievoorziening in het derde kwartaal van 2015 is de capaciteit voor informatiemanagement in gemeente Oegstgeest weer op het gewenste niveau. Vanaf dat moment is er meer capaciteit beschikbaar t.b.v. informatiebeveiliging. Dit is ook zichtbaar in de verbeteringen die de gemeente (ook in relatie tot dit datalek) is gestart.

Een nieuw (regionaal) informatiebeveiligingsbeleid is in wording. Dit beleid is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten waar elke gemeente zich aan heeft geconformeerd. De planning is dat dit beleid in het derde kwartaal van 2016 in de gemeente Oegstgeest wordt vastgesteld. Dit beleid zal al het vigerende beleid t.a.v. informatieveiligheid in Oegstgeest vervangen (waaronder het informatieveiligheidsbeleid en –plan uit 2005, het regionale Statuut Informatiebeveiliging uit maart 2013 en de Governance en incidentenprocedure gemeente Oegstgeest 2016). Het beleid heeft als doel de informatieveiligheid van de gemeenten in de regio te laten voldoen aan de BIG en veiligheidsrisico's tot een minimum te beperken.
In onderstaande tabel zijn de drie risico's opgenomen die kunnen leiden tot het ontstaan van een soortgelijk datalek als het datalek dat op 25 februari 2016 is geconstateerd.

Vervolgens is aangegeven welke maatregelen reeds zijn genomen om deze risico's te beperken en of deze maatregelen afdoende zijn om herhaling van dit type datalek te voorkomen.

Risico (i.r.l. datalek)	Maatregel	Startdatum	Status	Wel/Niet afdoende
Bestanden met persoonsgegevens t.b.v. werkzaamheden door leveranciers op andere apparatuur (bv USB, Laptop oid) zetten dan Servicepunt71 apparatuur.	1. Bewerkersovereenkomsten met leveranciers verscherpt. 2. Veranderde manier van werken waardoor leverancier alleen nog maar in de Servicepunt71 omgeving mag werken voor beperkte tijd en met strikte, minimaal benodigde toegang. 3. Bewustwording bij eigen medewerkers over de risico's hiervan	1. Eind 2015 gestart. 2. Sinds 2012 ingevoerd. 3. Eind 2015 gestart.	1. In uitvoering. 2. Ingevoerd. 3. In uitvoering.	1. Op papier afdoende, uitvoeringsprocessen voor controle hebben nog afzonderlijke aanscherping nodig. 2. Ja, afdoende 3. Ja, maar voortdurende herhaling blijft nodig.
Bestanden met persoonsgegevens t.b.v. werkzaamheden door leveranciers mailen.	1. Bewerkersovereenkomsten met leveranciers verscherpt. 2. Bewustwording bij medewerkers over de risico's hiervan.	1. Eind 2015 gestart. 2. Eind 2015 gestart.	1. In uitvoering. 2. In uitvoering.	1. Op papier afdoende, uitvoeringsprocessen voor controle hebben nog afzonderlijke aanscherping nodig . 2. Ja, maar voortdurende herhaling blijft nodig.
Bestanden met persoonsgegevens t.b.v. werkzaamheden door leveranciers in een cloudoplossing zetten (bv Wetransfer).	1. Bewerkersovereenkomsten met leveranciers verscherpt. 2. Bewustwording bij medewerkers over de risico's hiervan.	1. Eind 2015 gestart. 2. Eind 2015 gestart.	1. In uitvoering. 2. In uitvoering.	1. Op papier afdoende, uitvoeringsprocessen voor controle hebben nog afzonderlijke aanscherping nodig . 2. Deels, controle hierop is lastig

- **In hoeverre zijn de al ingezette verbeteringen voldoende om herhaling te voorkomen?**
- **Welke acties zijn aanvullend nodig om het herhalingsrisico tot een minimum te beperken?**

Uit het voorgaande blijkt dat de gemeente Oegstgeest in beleid en in contracten met de oud-leverancier aandacht heeft besteed aan betrouwbare gegevensverwerking door interne en externe medewerkers. In het contract met de oud-leverancier zijn hierover ook heldere afspraken gemaakt. Desalniettemin heeft het datalek dat op 25 februari 2016 is geconstateerd, kunnen ontstaan.

Dit leert dat het zeer van belang is om in beleid en contracten met leveranciers scherp te blijven op een betrouwbare gegevensverwerking en informatiebeveiliging en de wijze waarop dat gebeurt. Dit leert echter ook dat het vastleggen van handelswijzen en afspraken op papier onvoldoende garantie is dat een datalek niet zal ontstaan.

Dat een datalek niet voor 100% valt uit te sluiten, geldt voor alle gemeenten waaronder Oegstgeest. Een datalek kan op verschillende manieren ontstaan, waaronder ook het per abuis versturen van een verkeerde bijlage met persoonsgegevens naar de juiste persoon, of het versturen van de juiste bijlage met persoonsgegevens naar de verkeerde persoon. Geen enkel protocol of beveiligingssysteem kan een dergelijke menselijke fout voorkomen. Van belang is het dan ook dat aanvullend op de protocollen en afspraken met interne en externe medewerkers, voldoende bewustwording is van de risico's van gegevensverwerking en informatiebeveiliging.

Daarom is eind 2015 ook een traject gestart om bewustwording bij medewerkers over de risico's van gegevensverwerking en informatiebeveiliging te creëren.
In de kaderbrief van de directie voor 2016 geeft de directie de kaders aan voor de werkzaamheden en aandachtsgebieden van de teams en voor de doorontwikkeling van de organisatie in 2016 en verder. In de kaderbrief, die in 2015 is vastgesteld, wordt ook ingegaan een betrouwbare, actuele en tijdige informatiehuishouding:

> Om goed te kunnen sturen op verschillende lagen in de organisatie is het belangrijk dat we onze informatiehuishouding op orde hebben. Informatie dient betrouwbaar, actueel en tijdig beschikbaar te zijn, en op een eenvoudige manier te ontsluiten. In 2016 wordt een visie op informatievoorziening geformuleerd en een plan voor de komende tijd gemaakt wat aansluit op de visie.

Een combinatie van protocollen, afspraken en bewustwording kan wel leiden tot het aanzienlijk verminderen van de kans dat een datalek ontstaat. Hierop zet de gemeente Oegstgeest de komende tijd verder in.
Daarbij worden de bevindingen van de Visitatiecommissie Informatieveiligheid van de VNG (d.d. januari 2016) meegenomen. In januari heeft de Visitatiecommissie Informatieveiligheid onderzoek gedaan bij de gemeente Oegstgeest. De commissie heeft geconcludeerd dat de gemeente Oegstgeest zich het belang van informatieveiligheid voor haar dienstverlening beseft. Daarbij viel de Commissie specifiek positief op dat Oegstgeest op bestuurlijk en topambtelijk niveau doordrongen is van het belang van informatieveiligheid en gemotiveerd is om stappen voorwaarts te maken.
Tegelijkertijd zag de Commissie dat Oegstgeest:

- zich realiseert dat niet alle stappen tegelijk genomen kunnen worden en de gemeente werkt aan een uitvoerbaar programma dat op korte termijn eerste resultaten oplevert;
- daarbij nadrukkelijk aandacht heeft voor de verbinding tussen informatieveiligheid als onderdeel van het primaire proces en het perspectief voor ogen heeft dat informatieveiligheid waarde toevoegt aan de dienstverlening. De Commissie gaf aan ook voor deze benadering te staan.

In de toekomst wordt ook voorkomen dat – zoals eerder is gebeurd -een geboortedatum zichtbaar is in het venster van een envelop van de stempas. Dit kwam tijdens de informatiebijeenkomst d.d. 25 mei 2016 aan de orde.

Tevens kwamen die avond de volgende twee vragen aan de orde:

- Valt nog te achterhalen of er nog meer bestanden bij externe leveranciers 'zwerven'?
- Of en hoe kan de gemeente het downloaden van vertrouwelijke gegevens van computers van de gemeente onderzoeken en voorkomen?

Ten aanzien van de eerste vraag zal de gemeente de leveranciers aanschrijven die tot 2012 (toen een nieuwe manier van werken startte) applicaties leverden waarin persoonsgegevens van de gemeente Oegstgeest werden opgeslagen. In deze brief zal de gemeente, n.a.v. het datalek, aandacht vragen voor eventueel achtergebleven gegevens van de gemeente Oegstgeest op de apparatuur van (medewerkers van) de leveranciers. Wij vragen de leveranciers een check te doen binnen hun systemen en –indien aan de orde – gegevens van de gemeente Oegstgeest te verwijderen. Dit is de maximale inspanning die de gemeente kan leveren om te waarborgen dat er geen bestanden meer bij leveranciers beschikbaar zijn.

Ten aanzien van de tweede vraag worden maatregelen waar mogelijk getroffen, zoals beschreven in de tabel op pagina 5. Er zal altijd een afweging gemaakt moeten worden tussen werkbaarheid en veiligheid.

Zoals hierboven beschreven is de ontwikkeling ingezet dat in beleid, protocollen en afspraken met leveranciers steeds meer aandacht komt voor gegevensbescherming en informatieveiligheid. Dat in combinatie met een bewustwordingscampagne moet ertoe bijdragen dat de kans dat bestanden gaan 'zwerven' en vertrouwelijke gegevens worden gedownload sterk vermindert.