



## Vragen en antwoorden openbaarheid privacygevoelige gegevens

versie: 9 maart 2016 10:30 uur

### 1. Is er sprake van vrijkomen van persoonsgegevens?

Ja.

### 2. Welke gegevens zijn mogelijk naar buiten gekomen?

Gegevens vanuit de applicatie voor de gemeentelijke belastingen. Deze gegevens betreffen onder meer naam, geboortedatum, adresgegevens, geslacht en BSN-nummer van ongeveer ca. 6.500 inwoners van Oegstgeest (en 1.500 inwoners die vertrokken zijn uit Oegstgeest). 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.

### 3. Wanneer zijn er gegevens openbaar geweest?

Het vermoeden is dat de gegevens in januari en februari 2016 openbaar opvraagbaar zijn geweest, maar de exacte periode is moeilijk te achterhalen. Op 25 februari is de openbaarheid ontdekt en is de koppeling naar de gegevens onmiddellijk verwijderd.

### 4. Hoe kon het dat de gegevens naar buiten zijn gekomen?

Een oud-medewerker van een door Oegstgeest gecontracteerde applicatieleverancier heeft destijds vertrouwelijke informatie op zijn laptop opgeslagen. Hij heeft verzuimd deze op te schonen bij zijn uitdiensttreding. Deze informatie is door de koppeling van een netwerkschijf aan internet tussen januari en februari 2016 online benaderbaar geweest. Er lijkt sprake te zijn van een menselijke fout.

### 5. Als het om gegevens gaat van zo lang geleden, hoe kan het dan dat dat nu pas naar buiten is gekomen?

De netwerkschijf met gegevens is recentelijk, per abuis, verbonden met het internet. De gemeente heeft hiervan een melding gekregen op 25 februari. Daarna is meteen een onderzoek gestart. Het vermoeden is dat de gegevens in januari en februari 2016 openbaar raadpleegbaar zijn geweest, maar de exacte periode is moeilijk te achterhalen.

### 6. Hoe zeker zijn we dat niet eerder de gegevens naar buiten zijn gekomen?

We kunnen dat niet voor 100% uitsluiten.

### 7. Hoe is het ontdekt?

Een medewerker van een andere gemeente heeft een melding gemaakt bij de Informatie BeveiligingsDienst (IBD) van de Vereniging van Nederlandse Gemeenten.

### 8. Zijn de gegevens nog steeds openbaar?

Nee, direct na ontdekking is de netwerkschijf ontkoppeld van internet. De indexen van zoekmachines zijn geschoond.

### 9. Ik heb een brief ontvangen, wat voor risico loop ik?

U heeft een brief ontvangen omdat uw gegevens voorkomen in de computerbestanden die van buitenaf te benaderen zijn geweest. We kunnen niet uitsluiten dat dit gebeurd is.

Het kan zijn dat uw gegevens zijn benaderd. Hierdoor ontstaat het risico op misbruik van uw gegevens. Hierbij maken derden gebruik van valse of gestolen identiteitsgegevens. Ze kopen bijvoorbeeld spullen op naam van iemand anders zonder te betalen. We willen benadrukken dat officiële instanties bij aanvragen in vrijwel alle gevallen een kopie vragen van paspoort of rijbewijs, of van bankgegevens. Deze gegevens kwam niet voor in de computerbestanden.

Wij adviseren u om alert te zijn én te blijven. Hoe? Dat kunt u lezen op <https://www.politie.nl/themas/identiteitsfraude.html>

Op de site van de rijksoverheid over identiteitsfraude is meer informatie te vinden. [www.rijksoverheid.nl/onderwerpen/identiteitsfraude/documenten/publicaties/2015/12/02/geef-oplichters-geen-kans-een-veilig-id](http://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/documenten/publicaties/2015/12/02/geef-oplichters-geen-kans-een-veilig-id)

**10. Ik heb een brief ontvangen, wat voor risico kan ik in de toekomst nog lopen?**

Zie boven bij 9.

**11. Wat is identiteitsfraude?**

Identiteitsfraude is het opzettelijk misbruiken van identificatiemiddelen zoals persoonsgegevens of identiteitspapieren met de bedoeling daarmee een strafbaar feit te plegen. Voor nadere uitleg verwijzen we naar <https://www.politie.nl/themas/identiteitsfraude.html>

**12. Ik heb geen brief gekregen, maar mijn buurvrouw wel. Hoe kan dat?**

U heeft geen brief ontvangen omdat uw gegevens niet voorkomen in de gegevensbestanden die van buitenaf te benaderen zijn geweest.

**13. Betekent dit dat iedereen heel gemakkelijk de gegevens kon ‘googelen’?**

De betreffende bestanden waren vindbaar via online zoekmachines. Echter, bij een zoekresultaat was niet direct zichtbaar dat het om persoonsgegevens ging.

**14. Wie heeft het gedaan (schuldvraag)?**

Een oud-medewerker van een door Oegstgeest gecontracteerde applicatieleverancier.

**15. Wat is er gedaan na de constatering?**

De gemeente heeft direct het protocol en de procedures uitgevoerd die horen bij deze situatie.

Dit betekent:

- Er is direct onderzocht wat de situatie was en of het hier om privacygevoelige gegevens ging.
- Toen bleek dat dat laatste het geval was, is volgens protocol binnen 72 uur (in dit geval binnen 17 uur) na de eerste ontdekking melding gemaakt bij de Autoriteit Persoonsgegevens. De Informatie Beveiligingsdienst is op de hoogte gesteld.
- De netwerkschijf is in bewaring gesteld bij een notaris.
- De indexen van online zoekmachines zijn geschoond van de gegevens.
- Een gespecialiseerd bedrijf is ingeschakeld om uit te kunnen sluiten of de gegevens ook daadwerkelijk benaderd zijn van buitenaf.
- De betrokken personen zijn per brief geïnformeerd.
- De gemeenteraad is per brief geïnformeerd.

**16. Ik heb een brief gekregen over mijn persoonsgegevens. Wat kan ik doen?**

De gemeente adviseert u om extra alert te zijn op signalen van misbruik van uw persoonsgegevens. Het is van belang dat u extra alert bent op correspondentie en afschrijvingen die u niet kunt plaatsen. Op de site van de politie ([www.politie.nl/themas/identiteitsfraude.html](http://www.politie.nl/themas/identiteitsfraude.html)) staat meer informatie over het herkennen van signalen en hoe u misbruik kunt melden.

**17. Wat heeft de gemeente gedaan om mijn risico op schade te beperken?**

Zie eerdere vraag (15)

**18. Kan ik een nieuw Burgerservicenummer aanvragen?**

Nee, dat is niet mogelijk.

**19. Krijg ik een schadevergoeding?**

Nee, maar als u aantoonbaar schade heeft geleden, is het mogelijk om de gemeente aansprakelijk stellen.

**20. Treft de gemeente nu extra maatregelen?**

In lijn met de verscherpte wetgeving op het gebied van informatieveiligheid en gegevensbescherming is de gemeente al geruime tijd bezig met aanscherping van haar beleid. Zo worden onder andere hernieuwde afspraken gemaakt met alle leveranciers en verbonden partijen.

**21. Waar kan ik een klacht indienen?**

U kunt uw klacht indienen via <http://www.oegstgeest.nl/gemeente/producten-a-z/product-detail/producten/klachten/>

**22. Hoe stel ik de gemeente aansprakelijk?**

U kunt de gemeente aansprakelijk stellen als u door het openbaar worden van uw persoonsgegevens aantoonbare schade heeft geleden. Meer informatie over aansprakelijkstelling vindt u op de website van de gemeente Oegstgeest <http://www.oegstgeest.nl/gemeente/producten-a-z/product-detail/producten/aansprakelijkheid/>

**23. Relevante links**

- Informatie van de politie over identiteitsfraude <https://www.politie.nl/themas/identiteitsfraude.html>
- informatie van de rijksoverheid algemene informatie over identiteitsfraude [www.rijksoverheid.nl/identiteitsfraude](http://www.rijksoverheid.nl/identiteitsfraude)
- presentatie over identiteitsfraude [www.rijksoverheid.nl/onderwerpen/identiteitsfraude/documenten/publicaties/2015/12/02/geef-oplichters-geen-kans-een-veilig-id](http://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/documenten/publicaties/2015/12/02/geef-oplichters-geen-kans-een-veilig-id)
- filmpje over identiteitsfraude [www.rijksoverheid.nl/onderwerpen/identiteitsfraude/documenten/videos/2015/11/04/identiteitsfraude-voorkomen](http://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/documenten/videos/2015/11/04/identiteitsfraude-voorkomen)
- beleidsregels over datalekken [https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels\\_meldplicht\\_datalekken.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf)