ANTWOORD

VAN GEDEPUTEERDE STATEN

OP VRAGEN VAN

A.R. Witte (CU & SGP)
(d.d. 27 september 2019)

Nummer
3556

Onderwerp
Melding datalek 24 september 2019

Aan de leden van Provinciale Staten

Toelichting vragensteller
Op 24 september hebben een aantal leden van Provinciale Staten een brief ontvangen over een datalek in één van de provinciale systemen. Een alerte medewerker heeft op 11 september 2019 het datalek gemeld. Deze medewerker kon meer gegevens inzien dan voor de functie noodzakelijk. Na onderzoek bleek dat een andere groep van 406 behandelaren ook "zij het met wat meer moeite" meer gegevens kon inzien dan noodzakelijk. De provincie heeft zowel een melding gedaan bij de Autoriteit Persoonsgegevens als de betrokkenen middels een brief van 24 september op de hoogte gebracht. De provincie heeft dit datalek inmiddels 'gedicht'.

Volgens de Autoriteit Personeelsgegevens (website; geraadpleegd 27 september 2019) is de meldplicht afhankelijk van de (potentiële) impact van het datalek op de bescherming van persoonsgegevens en de persoonlijke levenssfeer van betrokkenen. "U hoeft een datalek niet te melden als het niet waarschijnlijk is dat het datalek leidt tot een risico voor de rechten en vrijheden van betrokkenen." De website van de Autoriteit Persoonsgegevens vermeld verder dat de betrokkenen (de personen van wie u gegevens verwerkt) alleen geïnformeerd hoeven te worden als "een datalek waarschijnlijk een hoog risico voor hun rechten en vrijheden oplevert."

1. *Aan hoeveel betrokken personen is de brief van 24 september verstuurd? Op hoeveel personen heeft dit datalek in totaal betrekking? Om welke groep(en) van personen gaat het?*

Antwoord
Er zijn brieven verstuurd aan de 42 personen wiens persoonsgegevens het betreft. Het zijn actieve en voormalige statenleden en fractiemedewerkers.

2. *Welke gegevens van deze personen konden door daartoe onbevoegde medewerkers van de ambtelijke organisatie worden ingezien? Hoe lang heeft dit datalek bestaan?*

Antwoord
Het betreft persoonsgegevens die de betrokkenen aan de provincie hebben verstrekt met oog op de salarisverwerking en het verstrekken van toegangspassen en IT-middelen. De werkwijze die geleid heeft tot het datalek is gevolgd sinds 16-02-2016.

Op 16-09-2019 is het systeem voor deze werkwijze gedeactiveerd en zijn alle persoonsgegevens van betrokkenen hieruit verwijderd.

3. *GS geeft aan dat het niet bekend is hoeveel medewerkers onbevoegd informatie heeft ingezien. Logt het systeem niet wie welke gegevens inziet? Zo nee, waarom niet?*

Antwoord
Het betreft een door de provincie aangeschaft standaard systeem van een van de marktleiders op het gebied van digitale ondersteuning van servicemanagement processen. Het is bedoeld voor het registreren en routeren van aanvragen en ondersteunt de afhandeling ervan. Het systeem registreert welke wijzigingen er tijdens de afhandeling van een aanvraag door wie worden aangebracht. Het systeem voorziet niet in een logging van personen die gegevens inzien zonder daar wijzigingen in aan te brengen.

4. *Hoe en op welke termijn, na hoeveel tijd, zijn door de medewerker, zijn afdelingshoofd, de functionaris gegevens bescherming, de concerndirectie, gedeputeerde staten, de Autoriteit Persoonsgegevens en uiteindelijk de betrokkenen op de hoogte gesteld? Wat is de tijdlijn? Kunt u in deze tijdlijn ook de maatregelen meenemen en om het lek te stoppen en de genomen maatregelen om de schade te beperken.*

Antwoord
De tijdlijn is als volgt geweest:

Actie	Toelichting
Melding door de medewerker	Op 11-09-2019 per e-mail gemeld maar door afwezigheid niet direct opgepakt. Op 16-09-2019 heeft de medewerker via het Datalekformulier gemeld, waarna direct de procedure voor het afhandelen van datalekken is gestart.
Inlichten afdelingshoofd	16-09-2019
Inlichten functionaris voor gegevensbescherming	16-09-2019
Inlichten concerndirecteur	16-09-2019
Inlichten gedeputeerde staten	16-09-2019 (gedeputeerde) 19-09-2019 (door gedeputeerde aan GS)
Maatregelen om het lek te stoppen	16-09-2019 Alle aanvragen zijn uit het systeem verwijderd en kunnen niet meer worden ingezien. De digitale aanmeldingsprocedure is gedeactiveerd. Er zijn procesafspraken gemaakt over de afhandeling van eventuele nog komende tussentijdse aanmeldingen. Tot er een oplossing is, zal dit niet via dit systeem worden uitgevoerd.
Melding bij de Autoriteit Persoonsgegevens	18-09-2019
Brief en email aan de betrokkenen verzonden	23-09-2019
Maatregelen om de schade te beperken	Om de betrokkenen in staat te stellen de nodige voorzorgsmaatregelen te nemen, zijn zij per brief

Actie	Toelichting
	geïnformeerd. In de brief wordt geadviseerd om alert te zijn op signalen van identiteitsfraude of ander misbruik van persoonsgegevens. Ook worden in de brief contactgegevens vermeld voor het stellen van vragen.

5. *Is er bij dit datalek binnen de wettelijke termijnen gehandeld? Zo nee, waarom niet?*

Antwoord
De Algemene Verordening Gegevensbescherming (AVG) schrijft voor dat de verwerkingsverantwoordelijke een inbreuk in verband met persoonsgegevens ('datalek') meldt zonder onredelijke vertraging en indien mogelijk uiterlijk binnen 72 uur nadat hij er kennis van heeft genomen. De datalekprocedure is gestart op 16-09-2019 en de melding aan de Autoriteit Persoonsgegevens is gedaan op 18-09-2019. Dit is binnen 72 uur nadat kennis is genomen van het datalek.

6. *Hoe is de ernst van dit datalek gekwalificeerd? Welke 'rechten en vrijheden' van personen zijn bij dit datalek in het geding?*

Antwoord
Het is altijd ernstig wanneer persoonsgegevens potentieel door ongeautoriseerde mensen benaderd kunnen worden. In deze specifieke situatie is geoordeeld dat de persoonsgegevens gezien hun aard gebruikt zouden kunnen worden bij vormen van (identiteits)fraude.

7. *Hoe is GS op grond van de inschatting van de 'ernst' van het datalek en de hoogte van het risico (zie vraag 6) tot de conclusie gekozen om: 1] een officiële melding bij de Autoriteit Persoonsgegevens te doen en 2] de betrokkenen over het datalek te informeren? Graag op beide onderdelen van deze vraag een apart gemotiveerd antwoord.*

Antwoord
1. Volgens het afwegingskader van de AVG is melding van een datalek aan de Autoriteit Persoonsgegevens nodig als er (a) sprake is een beveiligingsincident en (b) onrechtmatige verwerking redelijkerwijs niet is uit te sluiten.
   In dit geval is geoordeeld dat:
   (a) er sprake was van een beveiligingsincident, aangezien de vertrouwelijkheid van persoonsgegevens in dit aanmeldingsproces niet voldoende was geborgd. Namelijk, ook een aantal provinciemedewerkers die het systeem gebruiken voor andere ondersteunende taken dan de aanmelding van statenleden en fractiemedewerkers, konden met enige moeite kennis nemen van de betreffende persoonsgegevens.
   (b) onrechtmatige verwerking redelijkerwijs niet was uit te sluiten, omdat er geen logbestanden aanwezig zijn op basis waarvan met zekerheid is vast te stellen dat daadwerkelijk provinciemedewerkers onterecht kennis hebben genomen van de persoonsgegevens.

2. Op grond van de AVG dient de provincie aan betrokkenen mede te delen dat er sprake is geweest van een datalek, indien is vastgesteld dat het datalek waarschijnlijk een hoog risico voor betrokkenen inhoudt.
In dit geval is geoordeeld dat de persoonsgegevens gezien hun aard mogelijk gebruikt kunnen worden bij vormen van (identiteits)fraude én dat door ontbrekende logging niet is uit te sluiten dat de persoonsgegevens door te veel provinciemedewerkers zijn ingezien. Ondanks ons vertrouwen in de provinciale medewerkers en de verwachting dat zij zich integer gedragen, is besloten om betrokkenen per brief te informeren.

8. Welke leerpunten trekt GS uit dit datalek over de beveiliging van persoonsgegevens in de andere provinciale systemen?

Antwoord
Het optreden van dit datalek toont aan dat er continu aandacht nodig blijft voor het zorgvuldige omgaan met persoonsgegevens. Zowel in systemen die de provincie al meerdere jaren gebruikt als bij de aanschaf en inrichting van nieuwe systemen en het in gebruik nemen van nieuwe technologieën. We zetten de lijn door die we ingezet hebben. Begin dit jaar is een nieuwe bewustwordingscampagne gestart voor medewerkers, die nog steeds doorloopt. Op afdelingsniveau wordt regelmatig aandacht besteed aan het omgaan met persoonsgegevens. Tevens wordt er gewerkt aan een e-learning voor de medewerkers van PZH over informatieveiligheid en privacy. Daarbij is het bemoedigend dat onze aandacht voor bewustwording op dit onderwerp geleid heeft tot alertheid bij provinciale medewerkers, zoals in dit geval.

Den Haag, 15 oktober 2019

Gedeputeerde Staten van Zuid-Holland,
secretaris, voorzitter,

drs. H.M.M. Koek drs. J. Smit