Gemeente Utrecht

BEANTWOORDING SCHRIFTELIJKE RAADSVRAGEN 2021, NUMMER 308

Datum	26 januari 2022
Van	College B&W
Behandeld door	W. Langeveld, L. Meulman
Doorkiesnummer	14030
E-mailadres	Wijbe.langeveld@utrecht.nl, lotte.meulman@utrecht.nl
Kenmerk	9642429
Beleidsveld	Jeugd en Jeugdzorg

Geachte leden van de raad,

Hierbij ontvangt u de beantwoording van de schriftelijke raadsvragen jaargang 2021 nummer 308 van raadslid Gilissen (VVD) van 17 december 2021 over Bescherming persoonsgegevens door Samen Veilig Midden-Nederland.
De gestelde vragen zijn onderaan bijgevoegd.

Vraag 1
De VVD maakt zich zorgen over de werkwijze van SVMNL. Deelt het college deze zorg? Zo nee, waarom niet?

***Antwoord* 1**
Wij zijn geschrokken van het bericht over een nieuw datalek bij Samen Veilig Midden Nederland (SVMN). Wij hechten veel waarde aan bescherming van persoonsgegevens, zeker ook van de gegevens die door Samen Veilig Midden Nederland (SVMN) worden verwerkt. Dit zijn namelijk veelal gegevens van kinderen en gezinnen die zich in een kwetsbare positie bevinden. Een datalek bij SVMN kan grote impact op deze kinderen en gezinnen hebben. Ook met het oog op het eerdere datalek bij SVMN, dat in 2019 plaatsvond, verwachten we van SVMN uiterste zorgvuldigheid hierin.

SVMN heeft sinds het datalek in 2019, dat overigens van grotere omvang was dan het recente datalek, verschillende maatregelen genomen. Informatiebeveiliging staat bij SVMN hoog op de agenda. Zie hiervoor ook de antwoorden op vraag 5 en 6. In een reactie op het recente datalek geeft SVMN aan dat menselijke fouten in de regel de oorzaak zijn van datalekken. Dat snappen we, want waar mensen werken, worden fouten gemaakt. Maar dat maakt het voor de betrokkenen bij het recente datalek natuurlijk niet minder erg. Voor hen is elke mail met persoonsgevoelige informatie die per ongeluk wordt gestuurd aan iemand die deze informatie niet zou moeten ontvangen, er één te veel. Het is aan SVMN om de juiste maatregelen te nemen om datalekken zoveel mogelijk te voorkomen, zonder dat het voor medewerkers onwerkbaar wordt.

Wij zijn met het bestuur van SVMN in gesprek over de gegevensbescherming en nemen hier dit recente datalek ook in mee. Zie het antwoord op vraag 3 voor een toelichting op hoe we dat doen met behulp van de recent door de gemeente vastgestelde 'Strategische standaard gegevensbescherming, Risico's voor derde partijen'.

Vraag 2
Is het college het met ons eens dat bescherming van persoonsgegevens van cliënten - gezien de aard en gevoeligheid van de geleverde ondersteuning - absolute topprioriteit moet zijn voor SVMNL?

Antwoord 2
Ja. Zie ook het antwoord op vraag 1.

Vraag 3
Hoe oordeelt het college over de in het artikel genoemde gang van zaken?
Antwoord 3
Zie ook het antwoord op vraag 1.

We betreuren wat er is gebeurd en we zijn als opdrachtgever met SVMN in gesprek over de zaak en de opvolging daarvan, ook richting de getroffen cliënten. Daarnaast zijn we met SVMN in gesprek over gegevensbescherming in brede zin. We maken daarbij gebruik van de afgelopen november door de gemeente vastgestelde 'Strategische standaard gegevensbescherming, Risico's voor derde partijen'. De verwerkersverantwoordelijkheid ligt bij SVMN, maar omdat eventuele beveiligingsincidenten of datalekken bij hen ook negatieve consequenties voor de gemeente als opdrachtgever kunnen hebben, is het van belang daar met elkaar afspraken over te maken. De strategische standaard biedt handvatten om dat op een gestructureerde manier te doen, vanuit ieders rol en verantwoordelijkheid. Concreet willen we met SVMN een top 5 van risico's vaststellen, de passende maatregelen op deze risico's bepalen en afspraken maken over de opvolging van deze maatregelen.

De Autoriteit Persoonsgegevens (AP) en secundair de Inspectie Gezondheidszorg en Jeugd (IGJ) hebben als toezichthoudende instanties de expertise en het instrumentarium om formeel een oordeel te vellen over de informatieveiligheid en gegevensbescherming bij SVMN. SVMN heeft dit datalek - conform de geldende meldplicht- bij de AP gemeld. Wij hebben van SMVN begrepen dat de AP vooralsnog geen nadere actie heeft ondernomen naar aanleiding van de gedane meldingen. De IGJ heeft SVMN op 23 december, naar aanleiding van de berichtgeving in de media, ook enkele vragen gesteld over de gang van zaken. SMVN heeft zes weken de tijd om deze vragen te beantwoorden. Na ontvangst van die informatie beoordeelt de inspectie of er aanleiding is om verder onderzoek in te stellen. Wij volgen die ontwikkelingen nauwgezet. Als de AP en/of de IGJ tot de conclusie komt dat er sprake is van structurele problemen, dan zullen wij aanvullend actie ondernemen vanuit onze rol als opdrachtgever van SVMN.

In elk geval zijn de gemaakte excuses aan de getroffen cliënt op hun plaats.

Vraag 4
Is het college het met ons eens dat bij genoemde incidenten sprake zou kunnen zijn van een datalek? Zo nee, waarom niet?
Antwoord 4
Ja, ook volgens de definitie van de AP. Op het moment dat door een instantie als SVMN e-mails met vertrouwelijke informatie worden verzonden naar een derde die deze informatie niet behoort te ontvangen, is er sprake van een datalek. Om die reden heeft SVMN ook melding bij de AP gemaakt en betrokkene geïnformeerd.

Vraag 5
Is het college tevreden over de verbetermaatregelen die SVMNL heeft genomen na het grote datalek in 2019? Zo ja, waaruit blijkt dit?
Antwoord vraag 5
Zie antwoord vraag 6

Vraag 6
Welke maatregelen zijn door SVMNL genomen om te voorkomen dat informatie of persoonsgegevens in verkeerde handen komen? Hoe zit het met de naleving van deze maatregelen en kan het college bij SVMNL nagaan hoe vaak dit in de afgelopen 2 jaar is misgegaan?
Antwoord 5 en 6
Naar aanleiding van het datalek in 2019 heeft de gemeente Utrecht samen met de andere Utrechtse regio's opdracht gegeven aan het COT Instituut voor Veiligheids- en Crisismanagement om onderzoek te doen naar de afhandeling van het datalek en de status van de informatiebeveiliging bij SVMN. De

uitkomst van het onderzoek was dat SVMN in de afhandeling adequaat heeft gehandeld en dat de informatiebeveiliging beleidsmatig en organisatorisch was ingericht. Wel waren er wat betreft de implementatie daarvan nog stappen te zetten en daarvoor heeft het COT zes aanbevelingen gedaan, gericht op een balans tussen werkbaarheid en informatiebeveiliging. SVMN heeft vervolgens verschillende maatregelen genomen om de informatieveiligheid te verbeteren, in lijn met de aanbevelingen van het COT. Zij hebben het bureau Fox-IT, een gespecialiseerd bureau voor cybersecurity, ingehuurd om hen te ondersteunen bij de opvolging van het datalek.[1]

Het beleid van SVMN rond informatieveiligheid ziet er op hoofdlijnen als volgt uit: SVMN voert eens in de twee jaren een risicobeoordeling informatieveiligheid uit (2019, 2021). Op basis van de eerste risicobeoordeling is in 2020 een meerjarenprogramma opgesteld met maatregelen op diverse terreinen; kennis/bewustzijn, technische instellingen, organisatorische regelingen en governance. Het eerste jaar zijn maatregelen voor de risico's met de hoogste prioriteit ingevoerd, binnen een termijn van twee jaar maatregelen voor de andere benoemde belangrijke risico's. Het gaat onder meer om technische maatregelen, het ontwikkelen van archiefbeleid- en management van cliëntdossiers en het aanstellen externe functionaris gegevensbescherming. Om fouten, zoals het versturen van informatie naar verkeerde e-mailadres, zoveel mogelijk te voorkomen, is er in juli 2020 een bewustwordingscampagne informatieveiligheid gestart. Het eerste deel liep tot maart 2021. SVMN onderzoekt wat het effect is van deze campagne, op het voorkomen van datalekken en op het zorgvuldiger omgaan met informatieveiligheid. In januari 2022 brengt SVMN het onderdeel van de bewustwordingscampagne over zorgvuldig mailen en het gebruik van Zivver opnieuw onder de aandacht van de medewerkers. Een stuurgroep Informatieveiligheid bewaakt de sturing op het programma. Tevens worden stappen gezet voor het verkrijgen van het een NEN7510 light certificaat voor informatiebeveiliging.

Hoewel dat wel het uiteindelijke doel is, resulteert veel aandacht voor informatiebeveiliging niet per definitie direct in minder (of geen) datalekken. In 2019, 2020 en 2021 waren er respectievelijk 64, 84 en 68 interne meldingen van veiligheidsincidenten (met betrekking tot informatiebeveiliging) bij SVMN (voor het gehele werkgebied van SAVE in heel Utrecht-Flevoland en Veilig Thuis voor alle Utrechtse regio's, waar ca 700 fte werkzaam is), waarvan de datalekken conform geldende regelgeving zijn beoordeeld en zo nodig ook zijn gemeld bij de AP en betrokkenen.[2] *In 2019, 2020 en 2021 zijn er respectievelijk 9, 22 en 16 datalekken gemeld bij de AP. De stijging in 2020 kan volgens SVMN worden verklaard vanuit het toegenomen thuiswerken (ze zien relatief veel melding in maart, april en september) en later in het jaar een grotere bekendheid met het fenomeen datalek en de meldroute door de bewustzijnscampagne informatieveiligheid en de daaruit volgende meldingsbereidheid. Een stijging van het aantal gemelde datalekken is gebruikelijk na een bewustzijnscampagne en is vaak ook zichtbaar bij andere organisaties die aandacht besteden aan bewustwording. De insteek is dat er maatregelen worden getroffen op basis van de gemelde datalekken en dat het aantal meldingen daardoor uiteindelijk weer daalt.*

We zien we dat informatiebeveiliging hoog op de agenda staat bij SVMN. Dat is wat ons betreft terecht en daar houden we als opdrachtgever hen ook scherp op, onder andere in de kwartaalgesprekken die we voeren. De komende tijd gaan we ons gesprek met SVMN over informatiebeveiliging verdiepen met behulp van de eerdergenoemde strategische standaard. Zoals eerder aangegeven hebben de toezichthouders de expertise en het instrumentarium om een formeel oordeel over de informatieveiligheid bij SVMN te vellen. Dat geldt voor het recente datalek, maar ook voor de genomen maatregelen naar aanleiding van het datalek in 2019. De AP heeft zich in augustus 2019 uitgebreid laten informeren over de verbeterstappen en daarna de zaak rond het datalek afgesloten. In 2020 heeft de AP gevraagd om uitleg over een aantal meldingen. Wij begrijpen van SVMN dat deze uitleg is gegeven en dat de AP hierop geen verdere actie heeft ondernomen. De IGJ heeft eind 2019, volgend op een toezichtsbezoek aan SAVE met als thema e-health, ook aanbevelingen betreffende informatiebeveiliging gedaan. De opvolging van deze aanbevelingen was door de IGJ tot op heden nog niet getoetst. Naar aanleiding van het recent gemelde datalek heeft de IGJ de stand van zaken opgevraagd bij SVMN. Het vervolg hierop zullen we -zoals aangegeven- volgen.

---

[1] Zie ook de raadsbrief van 17 april 2019 hierover via iBabs Online

[2] Bij een veiligheidsincident wordt er onderzoek gedaan of er als gevolg van dit incident ook sprake is geweest van een datalek en welke risico's voor betrokkenen dit datalek heeft opgeleverd. Indien er beoordeeld wordt dat er (mogelijk) sprake is van een privacy risico voor de betrokkenen, is het melden aan de Autoriteit Persoonsgegevens verplicht.

Vraag 7
Is het college bereid SVMNL om opheldering te vragen over de gang van zaken? Zo nee, waarom niet?
Antwoord 7
Ja, daartoe zijn we bereid. Naar aanleiding van de recente berichtgeving in de media en deze raadsvragen hebben we SVMN om een toelichting gevraagd op zowel het recente datalek als het structurele beleid rondom informatieveiligheid. De uitkomsten van die gesprekken zijn waar relevant meegenomen in de beantwoording van deze raadsvragen. De komende tijd gaan we aan de slag met het vaststellen van de top 5 van risico's, het bepalen van de passende maatregelen en het maken van afspraken over de opvolging, conform de eerdergenoemde 'Strategische standaard gegevensbescherming, Risico's voor derde partijen'. Zie ook de antwoorden op de vragen 1, 3, 5 en 6.

Hoogachtend,
Burgemeester en wethouders van Utrecht,

de secretaris, de burgemeester,

Schriftelijkevragen - Bescherming persoonsgegevens door Samen Veilig Midden-Nederland

17 december 2021

Vragen:

Vandaag verscheen een verontrustend bericht op RTV Utrecht dat Samen Veilig Midden-Nederland (SVMNL) nog steeds onvoldoende doet om de persoonsgegevens van ouders en kinderen te beschermen.[1] SVMNL kwam in 2019 nog in afspraak toen een groot datalek werd ontdekt waarmee meer dan 3.000 dossiers op straat kwamen te liggen.[2]

Uit de berichtgeving blijkt dat de SVMNL de zaken nog steeds niet in orde heeft. Begin 2020 heeft de organisatie nog uitleg moeten geven aan de Autoriteit Persoonsgegevens (AP) en onlangs meldde een advocaat zich bij RTV die het relaas doet over een moeder die meerdere malen gegevens van andere dossiers op haar mail ontving. Stukken die wel voor de moeder waren bedoeld werden naar voor haar onbekende e-mailadressen gestuurd.

De VVD maakt zich zorgen over de werkwijze van SVMNL en heeft de volgende vragen:

1. Deelt het college deze zorg? Zo nee, waarom niet?
2. Is het college het met ons eens dat bescherming van persoonsgegevens van cliënten - gezien de aard en gevoeligheid van de geleverde ondersteuning - absolute topprioriteit moet zijn voor SVMNL?
3. Hoe oordeelt het college over de in het artikel genoemde gang van zaken?

In het artikel van RTV Utrecht wordt een aantal voorbeelden genoemd waarvan mogelijk sprake zou kunnen zijn van een datalek.

4. Is het college het met ons eens dat bij genoemde incidenten sprake zou kunnen zijn van een datalek? Zo nee, waarom niet?
5. Is het college tevreden over de verbetermaatregelen die SVMNL heeft genomen na het grote datalek in 2019? Zo ja, waaruit blijkt dit?
6. Welke maatregelen zijn door SVMNL genomen om te voorkomen dat informatie of persoonsgegevens in verkeerde handen komen? Hoe zit het met de naleving van deze maatregelen en kan het college bij SVMNL nagaan hoe vaak dit in de afgelopen 2 jaar is misgegaan?
7. Is het college bereid SVMNL om opheldering te vragen over de gang van zaken? Zo nee, waarom niet

Gesteld door:

- Dimitri Gilissen, VVD

[1] https://www.rtvutrecht.nl/nieuws/3254763/datalekken-hardnekkig-probleem-bij-samen-veilig-en-veilig-thuis
[2] https://www.rtlnieuws.nl/tech/artikel/4672826/jeugdzorg-datalek-dossiers-kinderen-utrecht-email