AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

3SRRC11006564

Aangetekend
Minister van VWS
t.a.v. De Directieraad van het Rijksinstituut voor
Volksgezondheid en Milieu (RIVM)
Antonie van Leeuwenhoeklaan 9
3721 MA BILTHOVEN

RIVM 101-2020 DG

15106 2020

Cc: (10)(2e)

Datum
11 juni 2020

Ons kenmerk
(10)(2g)

Contactpersoon
(10)(2e)
070 (10)(2e)

Onderwerp
Verzoek om inlichtingen

Geachte directie,

In de bovengenoemde zaak bericht de Autoriteit Persoonsgegevens (AP) u als volgt.

1. Aanleiding

De AP heeft kennis genomen van een artikel van de NOS van 6 juni 2020 over een (mogelijk) datalek binnen de website Infectieradar.nl dat beheerd wordt door het Rijksinstituut voor Volksgezondheid en Milieu (RIVM).

Op maandag 8 juni 2020 heeft u deze (mogelijke) inbreuk aan de AP gemeld met meldingsnummer (10)(2g)

Artikel NOS

In het artikel van de NOS "*Lek in RIVM-coronasite: gegevens van gebruikers makkelijk in te zien*"[1] staat vermeld dat de site Infectieradar een ernstig datalek bevatte. Volgens het artikel was het mogelijk om ingevulde antwoordformulieren op medische vragen te achterhalen door het unieke nummer van acht cijfers, dat gegenereerd wordt bij elk ingevuld formulier, aan te passen in de adresbalk in de browser. Onbevoegden konden hierdoor inzage krijgen in de medische persoonsgegevens, e-mailadressen, geboortejaar en cijfers van de postcode van betrokkenen. Het artikel geeft aan dat de NOS op basis van een (geautomatiseerde) test binnen een paar minuten de antwoorden van 44 betrokkenen heeft kunnen achterhalen. Volgens het artikel was het tevens mogelijk om gericht naar de antwoorden van betrokkenen te zoeken, omdat de antwoorden gerangschikt waren op het e-mailadres van de gebruiker.

[1] J. Schellevis, 'Lek in RIVM-coronasite: gegevens van gebruikers makkelijk in te zien', NOS 6 juni 2020.

AUTORITEIT
PERSOONSGEGEVENS

Datum
11 juni 2020

Ons kenmerk
(10)(2g)

Het artikel vermeldt dat het lek al sinds de introductie van de Infectieradar bestond, namelijk op 17 maart 2020. Na de melding door de NOS heeft het RIVM de vragenlijst op 6 juni 2020 offline gehaald en heeft het RIVM aangegeven dat zij het probleem aan het oplossen is.. Tot slot staat in het artikel dat het RIVM heeft verklaard dat elke dag ingevulde formulieren werden geleegd.

Melding RIVM

In uw melding van 8 juni 2020 heeft u aangegeven dat een beveiligingsexpert en een journalist een voor iedereen onbekende zwakte heeft ontdekt in het vragenlijstsysteem Formdesk, wat het RIVM gebruikt voor het lopende onderzoek Infectieradar. Door gebruik te maken van deze zwakte konden deze personen de ingevulde vragenlijsten inzien van personen die zich hebben aangemeld en het e-mailadres van de indiener kunnen achterhalen. Het datalek heeft onder andere betrekking op bijzondere persoonsgegevens, namelijk gegevens over iemands gezondheid, aangezien onder andere gevraagd wordt om medicatie die gebruikt wordt tegen medische condities en of de gebruiker gezondheidsklachten heeft gehad in de afgelopen week. U geeft aan dat de (mogelijke) inbreuk 49 betrokkenen heeft getroffen, die zich hebben aangemeld om mee te doen aan het onderzoek in het kader van de Infectieradar. U heeft aangegeven dat het misbruik beperkt is gebleven tot de tests van de NOS en de onderzoeker en dat deze verklaard hebben de gegevens te vernietigen.

2. Vragen

Naar aanleiding van het bovenstaande verzoekt de AP u om antwoord te geven op de volgende vragen:

1 Per welke datum raakte het RIVM bekend met de kwetsbaarheid in het vragenlijstsysteem Formdesk?
2 Licht toe waarom het RIVM elke dag de ingevulde formulieren moest legen van de website en vanaf welk moment de ingevulde formulier elke dag werden geleegd?

Tijdens de plenaire vergadering van de Tweede Kamer op 9 juni 2020 heeft de Minister van Volksgezondheid, Welzijn en Sport (hierna: De Minister) aangegeven dat de aanmeldformulieren van 49 van de 55.000 personen zijn ingezien. Verder geeft de Minister aan dat uit logfiles blijkt dat er niet ook nog andere mensen inzage in hebben gehad. Uit het antwoord van de Minister op de vraag van Kamerlid (10)(2e) (10)(2e)), of de Minister met zekerheid kan zeggen dat in de dagen daarvoor niet is ingelogd en gegevens zijn bekeken, blijkt niet duidelijk hoe ver in de historie is gekeken op onbevoegde inzage.

3 Kan het RIVM aan de hand van logging uitsluiten dat eerder dan de op 6 juni 2020 ontdekte inbreuk misbruik is gemaakt van de kwetsbaarheid in het vragenlijstsysteem Formdesk? Motiveer uw antwoord.

Tijdens de plenaire vergadering van de Tweede Kamer heeft de Minister verder verklaard dat het beveiligingsrisico dat het datalek heeft veroorzaakt tijdens de pentest van het formulier is ontdekt en dat aan Formdesk is gevraagd een oplossing door te voeren. De Minister geeft aan dat de oplossing deels wel en deels niet is overgenomen. In het artikel van Nu.nl '*Minister legt lek Infectieradar bij ontwikkelaar, bedrijf reageert verbaasd*'[2] geeft het bedrijf Formdesk aan dat de kwetsbaarheid niet eerder aan het licht is gekomen

[2] 'Minister legt lek Infectieradar bij ontwikkelaar, bedrijf reageert verbaasd', Nu.nl 9 juni 2020.

AUTORITEIT
PERSOONSGEGEVENS

Datum
11 juni 2020

Ons kenmerk
(10)(2g)

en ook niet door het ministerie/RIVM is teruggekoppeld aan Formdesk. Formdesk lijkt zich niet te herkennen in de woorden van de Minister.

4 Licht toe door wie, wanneer het beveiligingsrisico is ontdekt en op welke datum het probleem/de oplossing aan Formdesk is doorgegeven? Motiveer uw antwoord aan de hand van stukken.
5 Licht toe wat wordt bedoeld met de verklaring van de Minister dat het beveiligingsrisico deels wel en deels niet is overgenomen door Formdesk?
6 Waarom is geen controle uitgevoerd op de maatregelen die Formdesk zou (moeten) treffen?
7 Welke andere maatregelen heeft het RIVM getroffen om de vertrouwelijkheid van de ingestuurde formulieren te waarborgen?
8 Welke maatregelen neemt het RIVM om een soortgelijk datalek in de toekomst te voorkomen?

Tot slot verzoekt de AP het RIVM een afschrift te verstrekken van de onderzoeksrapportage die door het RIVM is opgesteld naar aanleiding van het bovengenoemde datalek en een afschrift van de resultaten van de pentest.

3. Reactietermijn

De AP verzoekt u om **uiterlijk dinsdag 16 juni 2020** antwoord te geven op de hierboven genoemde vragen, en de resultaten van de pentest en de onderzoeksrapportage (indien reeds beschikbaar) aan de AP toe te zenden.

Een afschrift van deze brief stuurt de AP naar de Functionaris voor de Gegevensbescherming van het Ministerie van Volksgezondheid, Welzijn en Sport.

De AP vertrouwt erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend

(10)(2e)

(10)(2e)

(10)(2e)

Autoriteit Persoonsgegevens