Ministerie van Volksgezondheid,
Welzijn en Sport

Deze nota wordt met een Kamerbrief meegestuurd: **Nee**

Aan	Directeur OBP	Deadline: 30 december 2022

nota

Vernietiging kopie data die ontstaan tijdens het proces archivering Hotspot COVID-19

TER BESLISSING

Secretaris Generaal / plv. Secretaris Generaal
Dir Organisatie, Bedrijfsv en Personeel
Afd. CIO kern en informatiemanagement

Opgesteld door
5.1.2e

5.1.2e @minvws.nl

Datum
16 december 2022

Kenmerk

Uw kenmerk

Zaaknummer
1041518

Bijlage(n)
0

1. Aanleiding

In mei 2022 is de Data Protection Impact Analyse (DPIA) Hotspot COVID-19 vastgesteld. In advies van de FunctionarisGegevensbescherming (FG) is hierover het volgende opgenomen:

"*Ten aanzien van de bewaartermijn gelden de beginselen van noodzakelijkheid (artikel 8, tweede lid, van de EVRM) en dataminimalisatie (artikel 5, eerste lid, onder c, van de AVG). Deze beginselen eisen dat de verwerking zich tot het noodzakelijke beperkt. Daarnaast is van belang om te onderbouwen welke waarborgen er zijn dat verwijdering van de tijdelijke verzamelingen ook daadwerkelijk plaatsvindt.*"

Op dit moment worden er diverse proefmigraties uitgevoerd met productiedata, om zo zeker te kunnen zijn dat de migratiescripts zodanig zijn gebouwd dat alle documenten die onderdeel zijn van het Hotspot archief ook met de juiste bijbehorende metadata gearchiveerd kunnen worden in het archiefsysteem. In deze bewerkingsstap ontstaat een set kopie data. Om te voldoen aan de AVG willen we als project na iedere proefmigratie de kopie data verwijderen op alle locaties waar deze staan. Daarvoor willen we graag werken volgens door VWS vastgestelde procedures en gebruik maken van de juiste documenten ter verantwoording van de vernietiging. Verantwoording in de zin van waarom documenten zijn vernietigd, maar ook dat deze op de juiste wijze zijn vernietigd. Hiervoor zijn we in gesprek gegaan met de Chief Information Security Officer (CISO) en Privacy Officer (PO) van OBP en de Concern Chief Security Officer. Allen hebben aangegeven dat er op dit moment geen vastgestelde procedure is en ook geen standaard document voor het vastleggen en verantwoorden van het vernietigen van documenten. Dit betekent dat wij als project op dit moment geen data kunnen vernietigen, aangezien onduidelijk is welke waarborgen noodzakelijk zijn om te voldoen aan Artikel 32 lid 2 Algemene Verordening Gegevensbescherming (AVG) waar gesproken wordt over" *de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig*." Immers hoe tonen we aan dat data daadwerkelijk vernietigd moeten worden en dat dit op de juiste wijze is gebeurd?

Daarnaast hebben we nog een issue ten aanzien van de vernietiging van de kopie data. Van alle locaties wordt een back-up gemaakt door SSC-ICT. Bij navraag

blijkt dat het vernietigen in de back-up niet standaard is ingericht. Er dient onderzocht te worden of dit via een beveiligingsincident mogelijk is. Of vernietiging van de kopie data in de back-up door middel van een beveiligingsincident mogelijk is, is op dit moment nog niet helder. Wel is bekend dat een back-up na één jaar wordt vernietigd. Dat betekent dat de kopie data één jaar aanwezig blijft in de back-up, of wanneer de back-up na dat jaar teruggeplaatst moet worden, nog langer.

2. Geadviseerd besluit

- Akkoord geven op het voorstel vanuit het project om zelf de kopie data te verwijderen van de verwerkingslocatie.
- Akkoord op pragmatische aanpak voor opdracht tot verwijdering van de kopie data, door projectmanager in plaats van door directeur OBP.
- Akkoord dat de kopie data nog 1 jaar in de back-up blijft bestaan.
- Akkoord op het opstellen van een procedure met SSC-ICT om on opgemerkt kopie data weer terug te plaatsen.
- Opdracht geven aan de lijnorganisatie VWS voor opstellen van een procedure voor het vernietigen van data in het algemeen en bij behorende verantwoordingsdocumenten.
- Aansluiten bij het interdepartementaal initiatief om data in de back-up te kunnen vernietigen, indien daar vanuit de AVG aanleiding toe is. Vanuit VWS is 5.1.2e (Informatie Beveiliging) aangesloten bij dit initiatief, dat vanuit Binnenlandse Zaken wordt aangestuurd, als verantwoordelijke voor SSC-ICT.

3. Kernpunten

VWS dient de kopie data te vernietigen zodra deze niet meer benodigd zijn voor verwerking (conform de DPIA en Artikel 32 lid 2 AVG). Op dit moment ontbreekt echter een procedure voor de ingang en een formele verantwoording voor het vernietigen van data. Daarnaast is het vernietigen van de kopie data niet mogelijk in de back-up.

4. Huidige risico's kopie data en mitigerende maatregelen

a. Huidige risico's

Op dit moment zien wij voor het project de volgende risico's:

- Er is geen formeel verantwoordingsdocument voor het vernietigen van data op de tijdelijke verwerkingslocatie.
- Er is geen standaard proces voor het vernietigen van data dat gevolgd kan worden.
- Doordat de data om bovenstaande reden niet vernietigd wordt, wordt de hoeveelheid data die in de back-up terecht komt met de dag groter. En iedere dag blijft 1 jaar in de back-up aanwezig. Na dit jaar verdwijnen de data uit de back-up en zijn deze niet meer beschikbaar.
- Wanneer data op de tijdelijke verwerkingslocatie wordt vernietigd, is deze nog aanwezig in de back-up gedurende één jaar.
- Data in de back-up kan waarschijnlijk alleen door een security incident worden vernietigd.

- Wanneer data in de back-up niet vernietigd kan worden, bestaat het risico dat bij terugplaatsing van een back-up data die eerder op de verwerkingslocatie is verwijderd, daar weer terugplaatst wordt, zonder dat dit gesignaleerd wordt. De kans dat dit voor komt is vrij klein, maar niet uit te sluiten. Met als risico dat VWS alsnog data onder zich heeft, die zij niet zou mogen hebben.

Deze punten vormen een risico voor het project hotspot COVID-19, maar ook voor VWS als geheel. Immers:

- De verwerker van VWS, SSC-ICT resulterend onder het ministerie van Binnenlandse Zaken is niet in staat om invulling te geven aan één van de rechten van betrokkenen genoemde rechten: "verwijdering van documenten". Naast imagoschade kan dit VWS ook een boete opleveren van de AP (Autoriteit Persoonsgegevens). Hierbij is het wel de vraag of dit ook betrekking heeft op back-up bestanden.

Deze situatie is besproken met de 5.1.2e en de 5.1.2e Ook zij onderschrijven de beschreven risico's.

b. *Voorstel voor gedeeltelijk mitigeren van de risico's kopie data binnen de scope van het project*

- De experts binnen het project hotspot COVID-19 verwijderen zelf de data van de verwerkingslocatie en verantwoorden dit via bijgaand document. Door verwijdering zijn de kopie data niet vernietigd, maar niet langer toegankelijk.
- Vanuit praktisch oogpunt geeft de projectmanager van het project Hotspot de opdracht tot verwijdering van de kopie data. Dit als gedelegeerde van de directeur OBP is.
- De kopie data blijven 1 jaar in de back-up. VWS accepteert daarbij het risico dat de data na het terugplaatsen van een back-up als nog bij VWS staat. Om dit risico te mitigeren wordt door de CISO OBP en CISO Concern samen met SSC-ICT een procedure opgesteld rondom het terugplaatsen van back-ups. Bij het terugplaatsen van een back-up worden de data van de verwerkingslocatie van het project 5.1.2i Digitale overleggen uitgesloten. Alleen op verzoek van de directeur OBP zal op deze locatie data teruggeplaatst worden. Hiermee wordt voorkomen dat kopie data ongemerkt weer beschikbaar komt.

5. Toelichting

a. *Financiële en personele gevolgen*
Geen

b. *Juridische aspecten*
Op dit moment voldoet VWS niet aan de eisen die de AVG stelt aan het omgaan met data. Hiervoor zijn een aantal mitigerende maatregelen getroffen waarmee de risico's maximaal zijn beperkt. Deze zijn beschreven onder punt C, hierna.

c. *Afstemming (intern, interdepartementaal en met veldpartijen)*

De inhoud van deze nota is afgestemd met 5.1.2e (CISO OBP) en 5.1.2e (PO OBP) en zij onderschrijven de inhoud van deze nota.

Daarnaast is er op 8 december een overleg geweest over deze nota met de volgende personen: 5.1.2e (Kennisplein). 5.1.2e (Kennisplein), 5.1.2e (Programma Open Overheid), 5.1.2e (5.1.2e OBP), 5.1.2e (Informatie Beveiliging), 5.1.2e en 5.1.2 5.1.2e 5.1.2e (5.1.2e VWS). Tijdens dit overleg zijn de volgende besluiten genomen:

- Aangezien verwijderen op dit moment de beste optie is om de gegevens ontoegankelijk te maken, zal het project de kopie data op de verwerkingslocatie verwijderen. Uiteraard met verantwoording over de verwijdering.
- Projectmanager Hotspot COVID is gemandateerd om opdracht te geven tot verwijderen van de kopie data op de verwerkingslocatie (5.1.2h).
- Bestaand beleid, wordt door Informatie Beveiliging gedeeld met de projectmanager.
- Informatie Beveiliging stelt op basis van het voorstel van het project een document op waarmee het project het verwijderen van kopie data verantwoord.
- Vanuit de lijnorganisatie (Informatie Beveiliging en CISO en PO van OBP) wordt samen met SSC-ICT een procedure uitgewerkt om in geval van een terugplaatsing van de back-up te borgen dat er geen data teruggeplaatst wordt op de verwerkingslocatie 5.1.2h , tenzij dit gebeurt op verzoek van de directeur OBP.
- Verwijderen van data door het project start pas nadat het verantwoordingsdocument vanuit de lijnorganisatie is opgeleverd.

d. Gevolgen administratieve lasten
Het project Hotspot zal iedere verwijdering van kopie data moeten vastleggen.

6. Informatie die niet openbaar gemaakt kan worden
Deze nota gaan niet met een kamerbrief mee.