Deloitte.

Deloitte Forensic & Dispute Services B.V.
Gustav Mahlerlaan 2970
1081 LA Amsterdam
P.O.Box 58110
1040 HC Amsterdam
Netherlands

Tel: +31 (0)88 288 2888
Fax: +31 (0)88 288 9721
www.deloitte.nl

Memo

Van:
Deloitte Forensic & Dispute Services

Datum:
17 januari 2022

Aan:
Project Oak Tree

Onze referentie:
MIN00624-01

Onderwerp:
Technische uitwerking Project Oak Tree specifieke afspraken - Uitlezen gegevens mobiele telefoon

Inleiding

Deloitte Forensic & Dispute Services B.V. (hierna: Deloitte) voert in opdracht van het Ministerie van Volksgezondheid, Welzijn en Sport (hierna: VWS) een aanvullend onderzoek uit naar de inkopen van persoonlijke beschermingsmiddelen (hierna: PBM) in de periode 1 januari 2020 tot 1 juni 2021 door VWS en het Landelijk Consortium Hulpmiddelen (hierna: LCH). In het kader van deze opdracht heeft Deloitte medewerkers geïdentificeerd die mogelijk beschikken over relevante data voor het onderzoek. Dit memo zie specifiek op de gegevens uit de (zakelijke) mobiele telefoons van medewerkers van VWS.

Achtergrond

Op 5 augustus 2021 heeft Deloitte aan VWS een informatieverzoek gedaan met betrekking tot gegevens uit de (zakelijke) mobiele telefoons van specifieke medewerkers van VWS. Vervolgens heeft veelvuldig overleg plaatsgevonden over de wijze waarop Deloitte deze gegevens kan verkrijgen van VWS ten behoeve van het onderzoek, waarbij VWS voor aanvang van het onderzoek al gestart was met het veiligstellen en verwerken van de gegevens uit de (zakelijke) mobiele telefoons van VWS medewerkers in het kader van de Wet openbaarheid van bestuur (Wob). Deze werkwijze van VWS in het kader van de Wob komt niet overeen met de gebruikelijke werkwijze voor de gegevens van mobiele telefoons van Deloitte in forensische onderzoeken. Echter, op verzoek van VWS is de Wob-werkwijze van VWS inzake de (zakelijke) mobiele telefoons als startpositie gehanteerd. Daarnaast bleek dat niet voor alle geïdentificeerde medewerkers van VWS de gegevens van de (zakelijke) mobiele telefoons vanuit de Wob werkwijze beschikbaar zijn.

Op 2 december 2021 heeft Deloitte op basis van voortschrijdend inzicht een aanvullend informatieverzoek opgesteld voor het veiligstellen en aanleveren van gegevens uit de (zakelijke) mobiele telefoons van de medewerkers van VWS. Conform standaard-werkwijze van Deloitte is VWS hierbij verzocht om Deloitte in staat te stellen de gegevens op forensisch correcte wijze uit die mobiele telefoons veilig te stellen (**i**), vervolgens de potentieel relevante gegevens te selecteren (**ii**) en de geselecteerde gegevens aan te leveren in het kader van het feitenonderzoek naar de inkoop van persoonlijke beschermingsmiddelen (**iii**). Om tegemoet te komen aan de vereisten voor het onafhankelijke en onpartijdige onderzoek van Deloitte en de wensen van VWS heeft nader overleg plaatsgevonden om deze gegevens zo goed mogelijk in het onderzoek te kunnen betrekken. Dit memo is hiervoor een vastlegging.

Werkwijze en afspraken VWS

VWS hanteert in het kader van de Wob een procedure voor het veiligstellen van data in mobiele telefoons. Deze Wob-procedure voor de data in mobiele telefoons was al gestart voor aanvang van het Deloitte onderzoek. Uitgangspunt in die werkwijze is de vrijwillige medewerking van de medewerker van VWS. Het betreft in de Wob werkwijze overigens enkel de telefoons van leden van het MT en hoger binnen VWS, zodat niet alle medewerkers in deze procedure standaard worden meegenomen. Het verzoek van Deloitte ziet onder meer op informatie berustende bij medewerkers die niet standaard binnen de Wob-procedure van VWS vallen.

Deloitte.

De Wob-werkinstructies voor het veiligstellen van gegevens door VWS laten het initiatief voor het aanleveren van gegevens uit de mobiele telefoon bij de betreffende medewerker. De gegevens worden vervolgens door dezelfde medewerkers van VWS gefilterd (valideren op relevantie en privacy gevoelige gegevens).

In de periode vanaf augustus 2021 zijn gesprekken met VWS gevoerd over de wijze van veiligstellen en het verkrijgen van de relevante data voor het onderzoek. VWS heeft daarbij aangegeven binnen het onderzoek van Deloitte vast te willen houden aan de werkwijze Wob voor wat betreft de gegevens uit de (zakelijke) mobiele telefoons.

Voorgaande heeft geleid tot specifieke voor dit onderzoek gemaakte afspraken over het verkrijgen van de gegevens van de (zakelijke) mobiele telefoons en aanvullende afspraken over de medewerkers die nog niet binnen de standaard Wob-werkwijze van VWS vielen. De gemaakte afspraken wijken af van de reguliere en forensisch geaccrediteerde werkwijze van Deloitte. Deloitte biedt in de gemaakte afspraken slechts technische ondersteuning bij het veiligstellen en uitlezen van de telefoons en is niet betrokken bij het selecteren van data. De werkwijze voor de (zakelijke) mobiele telefoons wordt daarmee uitgevoerd door en onder verantwoordelijkheid van VWS.

Risico-afwegingen

Deloitte ziet in het door VWS gehanteerde proces enkele risico s voor het onderzoek. Het veiligstellen van informatie ruim na 1 juni 2021 (einde onderzoeksperiode), kent als risico dat berichten inmiddels onherroepelijk verwijderd zijn. Daarbij is een volgend risico dat het initiatief in het selecteren van mogelijk relevante gegevens bij de medewerkers zelf ligt, waarbij de medewerker bewust of onbewust onvolledig kan zijn in de aanlevering. Het kunnen inschatten of gegevens relevant zijn is bij uitstek een afweging die Deloitte wil maken. Deloitte is in de door VWS gekozen procedure slechts ondersteunend en is afhankelijk van de door VWS en haar medewerkers gemaakte keuzes.

Om dit risico van (on)bewuste verwijdering of weglaten van relevante gegevens te mitigeren, wordt voorgesteld een onderzoeker van Deloitte in gesprek met de medewerker van VWS te laten benoemen wat mogelijk relevant is, en aan de medewerker van VWS de vraag te stellen of meekijken tijdens het selecteren is toegestaan, om zo tot een meer zorgvuldige invulling van de onderzoekswensen tegemoet te komen. Tevens heeft Deloitte aan VWS voorgesteld dat een kopie van de uitgelezen (zakelijke) mobiele telefoons geëncrypt in de kluis op de gebruikelijke VWS locatie gedurende de loop van het onderzoek opgeslagen blijft, conform bestaande werkafspraken voor andere data sets. Hierbij blijft de vrijwillige medewerking van de medewerker VWS voorop staan, ook als later teruggegaan moet worden naar deze kopie.

Procedure

Op 20 december 2021 heeft VWS aan Deloitte gevraagd om de gemaakte afspraken op te nemen in een technische beschrijving van het werkproces voor het uitlezen van gegevens uit mobiele telefoons ten behoeve van de beoordeling door de beveiligings- en privacyfunctionarissen van VWS. De procedure voor het uitlezen van gegevens vanaf mobiele telefoons is op hoofdlijnen weergegeven in dit document en betreft enkel de technische kanten van dit proces. Dit memo is niet bedoeld als handvat voor het beoordelen van de inhoudelijke data, zoals het bepalen van potentiële relevantie.

De technische stappen zijn:

i. **Veiligstellen**

- De geïdentificeerde medewerker VWS (hierna: custodian) wordt uitgenodigd ten kantore van VWS. De locatie betreft de Hoftoren aan de Rijnstraat 50, 2515 XP in Den

Deloitte.

Haag.

- Aldaar zal de custodian in een vergaderruimte worden ontvangen door een medewerker informatieverzoeken Programmadirectie Nafase COVID-19, een (data-)specialist van Deloitte en een onderzoeker van Deloitte.

- De custodian zal zijn/haar (zakelijke) mobiele telefoon, inclusief toegangscode, overhandigen aan de specialist van Deloitte ten behoeve van het maken van een gegevensextract met gespecialiseerde hardware en software.

- Er wordt een Chain of Custody en Chain of Evidence documentatie gestart (het proces wordt hiermee zorgvuldig vastgelegd). De medewerker informatieverzoeken Programmadirectie Nafase COVID-19 ziet toe op het correct verlopen van de procedure.

- De custodian kan de procedure bijwonen of ervoor kiezen andere activiteiten te verrichten in afwachting van het maken van het gegevensextract.

- De specialist van Deloitte zal het telefoontoestel aansluiten op de gespecialiseerde hardware en software (Cellebrite UFED Touch 2) voor het maken van een gegevensextract. De specialist van Deloitte kiest de methode van extractie op basis van technische mogelijkheden die beschikbaar zijn voor het aangeboden toestel. Vaak zal dit een volledige (logische) extractie van gegevens inhouden.

- De gespecialiseerde hardware en software houden op zichzelf geen data vast, maar kunnen enkel worden ingezet voor het faciliteren van het maken van het gegevensextract uit de mobiele telefoon.

- Het gegevensextract wordt tijdelijk opgeslagen op een externe (USB) gegevensdrager van VWS die aangesloten is op de Cellebrite UFED Touch 2 hardware. Chain of Custody en Chain of Evidence documentatie voor de externe (USB) gegevensdrager wordt gestart en/of geactualiseerd.

- Na succesvolle afronding van het gegevensextract dienen de gegevens door gespecialiseerde software te worden geïnterpreteerd en doorzoekbaar gemaakt om tot een selectie van potentieel relevante gegevens te kunnen komen. De software voor het interpreteren van het gegevensextract zal worden gebruikt op een laptop van VWS die door Deloitte tijdelijk is ingericht met de gespecialiseerde software en corresponderende softwarelicentie en die het kantoor van VWS niet zal verlaten.

- Het proces van het interpreteren en doorzoekbaar maken van het gegevensextract op de laptop van VWS genereert zogenaamde case data. De case data wordt enkel bewaard op de externe (USB) gegevensdrager van VWS.

- Het telefoontoestel kan na opslag van het gegevensextract op de externe gegevensdrager van VWS worden geretourneerd aan de custodian. Chain of Custody en Chain of Evidence documentatie wordt geactualiseerd.

Deloitte.

ii. Selecteren

- Na het succesvol afronden van het interpreteren en doorzoekbaar maken van het gegevensextract door middel van de gespecialiseerde software, krijgt de custodian de gelegenheid om potentieel relevante gegevens voor het onderzoek te selecteren uit het gegevensextract.

- De onderzoeker van Deloitte geeft de custodian uitleg over de scope van het onderzoek en licht daarbij toe welk soort communicatie potentieel relevant is. De custodian wordt gevraagd of de onderzoeker mag meekijken. De onderzoeker maakt verslag op ten behoeve van het onderzoeksdossier, waarbij de custodian gevraagd wordt dit verslag te accorderen.

- Het selecteren door de custodian kan door het uitsluiten van niet-zakelijke communicatie uit het gegevensextract en/of door het insluiten van potentieel relevante zakelijke communicatie uit het gegevensextract.

- Het selecteren gebeurt door het geven van een label door de custodian aan gehele conversaties of door het insluiten of uitsluiten van individuele berichten uit conversaties uit het berichtenverkeer die zijn veiliggesteld in het gegevensextract.

- De custodian en de onderzoeker van Deloitte bespreken, indien mogelijk en gepast, samen de uitleg van de custodian waarom conversaties en/of berichten die niet zijn uitgesloten en niet zijn ingesloten, volgens de custodian niet in aanmerking komen voor verdere behandeling in het onderzoek.

- De geselecteerde conversaties en/of berichten worden opgenomen in een rapport formaat die de gespecialiseerde software kan genereren. Het rapport bevat naast generieke technische informatie over het telefoontoestel, enkel de door de custodian geselecteerde conversaties en/of berichten.

- Het rapport wordt opgeslagen op een separate en versleutelde externe gegevensdrager die voldoet aan de beveiligingswaarde voor het opslaan van gegevens met rubricering Departementaal Vertrouwelijk. Chain of Custody en Chain of Evidence documentatie voor de externe versleutelde gegevensdrager wordt gestart en/of geactualiseerd.

iii. Aanleveren

- De rapporten met geselecteerde conversaties en/of berichten uit het gegevensextract van de mobiele telefoons conform het informatieverzoek van Deloitte worden door VWS volgens de bestaande randvoorwaarden voor transport en overdracht, aangeleverd aan Deloitte.

- Tenzij anders overeengekomen met de custodian en/of VWS, zal Deloitte na verificatie van de ontvangen gegevens de instructie geven aan VWS voor het vernietigen van de gegevens op de externe (USB) gegevensdrager van VWS volgens procedure *NIST SP 800-88 Rev. 1* . Chain of Custody en Chain of Evidence documentatie wordt geactualiseerd.

- De laptop van VWS bevat geen gegevens uit de mobiele telefoon en blijft te allen tijde in beheer bij VWS.

Deloitte.

5
17 januari 2022

Gegevensdragers

VWS dient een laptop met het Microsoft Windows besturingssysteem ter beschikking te stellen aan Deloitte. Deloitte zal de laptop voorzien van de benodigde gespecialiseerde software. De laptop behoeft geen toegang tot het internet. Deloitte heeft administrator toegangsrechten nodig om de gespecialiseerde software te kunnen installeren en gebruiken. Door het proces van genereren van een gegevensextract van een mobiele telefoon worden geen gegevens uit de mobiele telefoon op de laptop geplaatst. In de technische procedure voor het veiligstellen, selecteren en aanleveren van potentieel relevante berichten uit mobiele telefoons, zijn er (tenminste) twee gegevensdragers nodig:

1. Een externe (USB) gegevensdrager voor het tijdelijk bewaren van het gegevensextract en case data. Deze gegevensdrager blijft in beheer bij en door VWS. De gegevens op deze gegevensdrager worden na afloop van de procedure vernietigd door VWS.

2. Een tweede versleutelde (USB) gegevensdrager die wordt gebruikt voor het opslaan van de rapporten met de geselecteerde conversaties en/of berichten. Deze gegevensdrager kan eveneens worden gebruikt voor het transporteren van de gegevens naar de datacenter faciliteiten van Deloitte in Amsterdam conform eerder afgesproken wijze. De gegevensdrager dient te voldoen aan de beveiligingswaarde voor het opslaan van gegevens met rubricering Departementaal Vertrouwelijk.