

Beste 5.1.2 en 5.1.2.e
2e

Zoals jullie bekend is hebben wij enige tijd een tweetal klachten ontvangen over het gebruik van de tool OBI4WAN ihkv Social media monitoring. De klachten behelsden voornamelijk een schending van actieve informatieplicht op grond van artikel 14 AVG.

Om inzicht te krijgen in de verwerking heb ik samen met mijn collega 5.1.2.e en ik, gesproken met 5.1.2.e en ik heb meegekeken met 5.1.2.e in de applicatie OBI4WAN. Ook heb ik bij de mediadesken nagevraagd of zij beide 'klagers' kennen. Slechts de helft van de mediadesken heeft gereageerd. Van een mediadesk kregen we zelf de opmerking dat het te veel werk was en ze derhalve geen gehoor zouden geven aan het verzoek.

Uit het inzicht dat wij bij de behandeling van de klachten hebben verkregen leiden wij af dat we een aantal privacy-risico's lopen. Hieronder zal ik geconstateerde de risico's benoemen met het verzoek om hier actie op te ondernemen.

1. Op de verwerking van de Brandmonitor (jullie Social media werkzaamheden ihkv AVG gerelateerde analyses etc..) is in 2017/2018 een GEB gedaan. Van deze GEB zijn verschillende versies in omloop, ik heb er al 2, die inhoudelijk ook van elkaar verschillen. Uit de GEB komt naar voren dat de grondslag van de verwerking (vermoedelijk) onjuist is vastgesteld, ook de genoemde bewaartermijn van 10 jaar achten wij – zonder nadere onderbouwing – onnodig lang. Ook blijkt niet dat er na 2018 nog een her-evaluatie van de verwerking heeft plaatsgevonden. Dit leidt tot risico's in de rechtmatigheid van de verwerkingen en dataminimalisatie.
2. Hoewel op de verwerking een GEB is gedaan is deze verwerking toen alle verwerkingen in 2020/2021 ihkv het programma Privacy in de bedrijfsvoering de verwerkingen van Communicatie in kaart zijn gebracht niet naar voren gekomen. Hierdoor is de verwerking niet opgenomen in ons verwerkingsregister. Dit leidt tot een risico dat wij onze verantwoordingsplicht niet na kunnen komen.
3. Tijdens een inkijkje in de tool OBI4WAN kreeg ik niet de indruk dat de AVG (brandmonitor) verwerkingen waren gescheiden van de Wpg (ondersteuning politietraak) verwerkingen. Noch dat duidelijk was welke query's voor welke werkzaamheden zijn opgevraagd. Ook Hierdoor bestaat het risico dat we geen correct gevolg kunnen geven aan het inzageverzoek op grond van de AVG en Wpg.
4. In sommige gevallen, voor zover ik heb kunnen achterhalen is dit in beperkte mate, worden de query's gedownload naar een excelsheet. Hierbij ontstaat het risico dat we de excelsheet langer bewaren dan noodzakelijk, dat er personen bij de excelsheets kunnen die hiertoe niet bevoegd zijn en dat we hierdoor ook niet correct kunnen voldoen aan het inzageverzoek op grond van de AVG en Wpg,
5. Uit ons extern privacy statement blijkt onvoldoende voor welke doelen (AVG en Wpg) wij Social Media monitoring inzetten. Hiermee schenden we het transparantiebeginsel en de informatieplicht. Ik heb van jullie begrepen dat jullie al werken aan een tekstvoorstel om dit risico te mitigeren. Het tekstvoorstel kun je mailen naar: 5.1.2.i @politie.nl. De e-mail komt dan bij de afdeling Privacy & Compliance van het PDC terecht. Zij (wij) zijn de beheerders van het privacy statement en zullen dit dan meenemen in de volgende aanpassing van het privacy statement.
6. Naar aanleiding van de ontvangen klachten is gebleken dat Spotler zelf een inzageverzoek heeft behandeld als ware zij verwerkingsverantwoordelijke. Uit artikel 12.2 van de verwerkersovereenkomst blijkt dat als zij zelfstandig een inzageverzoek ontvangen zij met de verwerkingsverantwoordelijke hierover overleg dienen te voeren. De vraag is even of de afhandeling van het inzageverzoek door Spotler op een juiste wijze is afgehandeld en vanuit welke rol als verwerkingsverantwoordelijke zij dan de betrokken persoonsgegevens aan ons hebben verstrekt. Wellicht dat een en ander klopt, maar om het risico uit te sluiten dat er op een onjuiste wijze uitvoering is gegeven aan het inzageverzoek lijkt het me zinvol dat hier een keer over wordt gesproken.
7. Zoals aangegeven is eind 2022 een GEB gedaan op de tool OBI4WAN in het kader van de Social media accounts die onze collega's beheren en ihkv webcare. In het verwerkingsregister staat een verwerking genaamd : Uitvoeren onderzoek publiek toegankelijke bronnen. Deze verwerking behoort ofwel toe aan het Operationeel Centrum ofwel aan Intelligence. Het is mij niet duidelijk of jullie aan de politietraak ondersteunende werkzaamheden hierin zijn geborgd. Mocht dat niet het geval zijn lopen we het risico dat de verwerking niet volledig in kaart wordt gebracht en we een of meer van de voorgaande risico's lopen.

Om een aanvang te maken voor een her-evaluatie van de verwerking rondom de Brandmonitor en de ingeschatte risico's te kunnen mitigeren wil ik jullie verzoeken bijgaand formulier:

<https://agora.portal.politie> 5.1.2.i

In te vullen. Ik weet dat het formulier een aantal verplichte invulvelden heeft ten aanzien van betrokken personen. In deze velden kun je dan mijn naam vermelden.

Na de ontvangst van dit formulier treden wij in contact met jullie om de verwerking uit te lopen en kijken over welke privacy risico's – behalve nummer 7 – we kunnen adviseren.