DPG-Raad

d.d.: 22-10-2021	**Agendapunt 04**
Onderwerp:	**Mandaat Security Operation Center**
Strategisch thema:	Informatievoorziening/informatiebeveiliging
Portefeuillehouder:	[redacted]
Opgesteld door:	[redacted]
Overlegd met:	[redacted]
Status:	Ter instemming
	DPG-RAAD
Voorgestelde beslispunten:	- De DPG-Raad wordt gevraagd in te stemmen met de uitbreiding van de opdracht aan het SOC.
Aanleiding:	Na de datadiefstal van eind januari heeft de DPG-raad met een aantal maatregelen ingestemd teneinde de informatiebeveiliging te intensiveren. Eén van die maatregelen vormde de inzet van een Security Operation Center (SOC) dat het gebruik van de systemen CoronIT en HPzone(Lite) screent en de logfiles op afwijkend gedrag controleert. Afwijkingen worden vervolgens onderzocht en indien benodigd worden hierop maatregelen getroffen nadat met de betreffende werkgever (DPG of landelijke partner) in contact is getreden. Inmiddels wordt het SOC ook meer en meer bevraagd en benut in gevallen van (verdenkingen) van fraude zowel door de GGD'en als ook door politie en OM. Dit vraagt om een uitbreiding van de opdracht, en daarmee mandaat van het SOC, teneinde medewerking te geven aan dergelijke verzoeken. De DPG-raad wordt gevraagd om in te stemmen met de uitbreiding van de opdracht aan het SOC en de eigen CISO/informatiemanager evenals FG hierover te informeren.
Beoogd resultaat:	• Effectieve fraudebestrijding • Geformaliseerd mandaat/bevoegdheden SOC • Waarborgen rondom de bejegening en privacy van medewerkers
Argumenten:	Nu in Nederland gewerkt wordt met QR codes om toegang te krijgen tot diverse accommodaties en activiteiten, is het belang om als positief getest en/of gevaccineerd in de systemen te staan toe. Dit leidt ertoe dat mensen ook oneigenlijke wegen bewandelen of medewerkers onder druk zetten om al dan niet tegen betaling valse registraties te doen. In diverse GGD'en speelt dit momenteel en ook de politie krijgt hierover steeds vaker signalen binnen. Deze signalen willen we nader onderzoeken om dergelijke fraude een halt toe te roepen en te voorkomen dat er valse QR-codes in omloop komen. Voor dergelijk onderzoek is toegang tot o.a. onze logfiles, via het SOC benodigd.

	Het SOC dient echter secuur af te wegen of zij wel of niet aan dergelijke verzoeken gehoor kan gegeven, gezien de juridisch context waarbinnen zij dient te acteren. In bijgevoegd stappenplan is zichtbaar gemaakt, hoe de context gewogen dient te worden en wanneer het SOC wel/niet haar medewerking kan geven.
Financiële, personele en juridische consequenties:	• De kosten van het SOC, evenals de uitbreiding als gevolg van de verbreding van haar taak worden volledig gedekt uit de DVO. • Iedere GGD heeft aan haar OR instemming gevraagd voor de werkzaamheden van het SOC. Vervolgens zijn medewerkers zijn geïnformeerd over het bestaan van het SOC en de screening die op hun accounts in de systemen CoronIT en HPzone(Lite) plaatsvindt. • Bijgevoegd stappenplan is bedoeld om inzicht te geven in de zorgvuldige afhandeling van verzoeken door het SOC.
Eerder genomen besluiten:	- Instelling van het SOC - Instemmingsverzoek aan iedere OR rondom SOC
Bijlagen:	- Stappenplan toetsing externe verzoeken