Aanleiding

In 2020 is op meerdere momenten aandacht geweest voor gegevensbescherming bij testen, traceren en vaccineren. Op 16 september 2020 berichtte bijvoorbeeld Nieuwsuur dat medewerkers van de GGD inzage hebben in alle persoonsgegevens die ten behoeve van testen en traceren zijn opgeslagen. De Autoriteit Persoonsgegevens heeft naar aanleiding hiervan informatie gevraagd over de verwerking en bescherming van persoonsgegevens. De gevraagde informatie is door de GGD aan de Autoriteit Persoonsgegevens verstrekt. Op 3 november 2020 berichtte het AD dat medewerkers van de GGD zichzelf ongeoorloofd toegang hebben verschaft tot de persoonlijke gegevens van bekende personen die geregistreerd staan in het IT-systeem. In reactie op deze signalen meldt de GGD dat alle callcentermedewerkers bij alle dossiers kunnen omdat ze de informatie van mensen die bellen voor een afspraak moeten kunnen controleren en dat medewerkers een geheimhoudingsverklaring moeten ondertekenen en dat er scherp gecontroleerd wordt op wie wat doet in het systeem.

Naast dat op elk signaal is gehandeld hebben deze signalen en incidenten ertoe geleid dat in november de Regiegroep Digitale Ondersteuning Test- en Traceerketen (DOTT) is ingericht en is besloten door VWS, GGD GHOR Nederland en het RIVM tot het uitvoeren van een gezamenlijke risicoanalyse op 'de IT-systemen en gegevensuitwisseling in de test- en traceerketen Covid-19'. De analyse is in zeer korte tijd uitgevoerd aan de hand van interviews en het doornemen van documentatie. Er is geen audit uitgevoerd. Over de resultaten van de risicoanalyse is de Kamer bij brief geïnformeerd op 24 december. In overleg met het Nationaal Cyber Security Center (NCSC) is besloten om het rapport zelf om veiligheidsredenen niet openbaar te maken. Naar aanleiding van de risicoanalyse heeft de voorzitter van de LCT de Regiegroep DOTT opdracht gegeven tot het opstellen van een ketenbreed verbeterplan. 5.1.2e Het concept verbeterplan wordt in de week van 1 februari besproken in de LCT.

Sinds 24 januari zijn er meerdere berichten verschenen over mogelijke datadiefstal bij de GGD'en. Een journalist van RTL heeft bekend gemaakt dat mensen die voor de GGD'en werken datasets met persoonsgegevens uit GGD-systeem HPZone online te koop hebben aangeboden, en persoonsgegevens van individuele personen uit CoronIT te koop aanbieden.

De voorzitter van GGD GHOR Nederland heeft de minister van VWS gevraagd of deze expertise kan leveren om ondersteuning te bieden bij de uitwerking van de te nemen maatregelen en de implementatie daarvan. Deze steun is toegezegd in de vorm van een team experts (kernteam) tenminste kennis aanwezig is van privacy en informatiebeveiliging en waarin GGD GHOR Nederland de inhoudelijke expertise levert. Het team heeft als opdracht om de GGD GHOR en de GGD'en bij te staan in het analyseren van risico's ten aanzien van informatiebeveiliging en privacy (zowel in techniek als in proces en organisatie), concrete voorstellen voor verbetering te doen en te helpen bij implementatie waar nodig.

Direct na het bekend worden van de mogelijke handel in persoonsgegevens is door VWS ook met GGD GHOR Nederland afgesproken dat onder verantwoordelijkheid van VWS zou worden gestart met een "Red Team". Dit is de naam voor een aanpak om de digitale verdediging van een organisatie en van systemen te testen. Gebleken is dat het team er in is geslaagd om zich toegang te verschaffen tot documenten die niet beschikbaar zouden moeten zijn. Hierop moet worden geacteerd. De documenten zijn niet meer beschikbaar omdat GGD GHOR de voorziening heeft afgesloten. Het team continueert ook de werkzaamheden.

In de week van 1 februari kwamen ook signalen over de DigiD-aansluiting van CoronIT. Deze voldoet aldus Logius (nog) niet aan de eisen. Om de aansluiting te behouden is aanpassing door de GGD nodig op korte termijn.

Tot slot is op 3 februari een Kamerdebat gevoerd over bovenstaande. In dit debat zijn toezeggingen gedaan die moeten worden opgevolgd.

Activiteiten VWS

Bovenstaande leidt tot een aantal aanvullende activiteiten van VWS:

- *Parlementair*
  Opvolgen toezeggingen, rapporteren aan de bewindspersonen en parlementair proces (Kamerbrieven, debatten, etc)

- *Samenstellen en begeleiden kernteam*
  Het toegezegde team experts moet worden samengesteld en begeleid in de hierboven beschreven opdracht.

- *Opvolgen incident gevonden door Red team*
  De NCTV deelt ons oordeel dat er zeer gevoelige informatie beschikbaar was en verkregen door het Red team die niet beschikbaar had moeten zijn. Er moet een forensische kopie worden gemaakt en onderzoek gestart. Hierbij zullen GGD GHOR, RIVM, NCTV, NCSC en politie betrokken zijn.

- *Opvolgen risico DigiD*
  BZK heeft hulp aangeboden aan GGD. Gezien het risico voor de opdracht van VWS ligt indien nodig extra hulp vanuit VWS voor de hand.

- *Verbinden activiteiten met ketenregie*
  Gezien de inhoud van de activiteiten ligt het voor de hand dat de voorzitter van de LCT structureel wordt geïnformeerd over de stand van zaken.

Aanpak

- *Programmadirecteur en programma opvolging verbetering informatieveiligheid en privacy*
  De activiteiten zullen programmatisch worden aangestuurd. 5.1.2e is bereid gevonden om de komende tijd als programmadirecteur de genoemde activiteiten aan te sturen, met uitzondering van de parlementaire activiteiten. Deze worden belegd bij PDC19 en DICIO. Een parlementair medewerker zal linking pin zijn naar het programma.

- *Stuurgroep*
  Het programma zal een stuurgroep kennen met daarin de 5.1.2e en 5.1.2e De minister zal structureel worden geïnformeerd over de stand van zaken.

- *Inbedding programma*
  Het programma heeft gezien de aard van de activiteiten DICIO als thuisbasis. Dagelijkse begeleiding zal plaatsvinden door de 5.1.2e

Bemensing

- *Programmateam*
  Voor het programma zal een secretariaat worden samengesteld. De inkoop en financiën worden ondersteund vanuit het al bestaande programma Realisatie Digitale Ondersteuning van DICIO. Voor het programmateam zullen ook een of enkele externe beleidsmedewerkers worden gezocht.

- *Expert team*
  De eerste kern van het expert team zal 5 februari worden geworven. Nu wordt tenminste gedacht aan:
  - Bijdrage van CIO Rijk en CISO Rijk
  - Bijdrage van NCSC/Z-Cert
  - Bijdrage van de diensten
  - Experts privacy en zorg via Hooghiemstra en partners
  - Experts informatieveiligheid van Noordbeek, NFIR, ...
  - Beschikbaarheid CPO VWS, CISO VWS, BVA VWS

- *Opvolging bevinding Read team*
  5.1.2e voorstel?