

Datadiefstal gegevens coronatesten

Dit weekend zijn twee medewerkers van de coronatest aangehouden op verdenking van datadiefstal. Zij zouden tegen betaling persoonsgegevens uit de GGD-systemen hebben aangeboden. Terwijl veel Nederlanders grote negatieve gevolgen van het coronavirus ondervinden, willen criminelen persoonlijk gewin halen uit de gegevens van mensen die zich laten testen. GGD GHOR Nederland heeft aangifte gedaan en de zaak is door de politie en het OM in behandeling genomen.

André Rouvoet, voorzitter GGD GHOR: “Wij zijn verantwoordelijk voor de veiligheid van onze systemen. Iedereen die zich bij ons laat testen moet daar op kunnen vertrouwen. Daarom zijn we onmiddellijk bezig om verdere maatregelen te treffen. Deze criminele activiteit is een klap in het gezicht van 17 miljoen Nederlanders, die allemaal lijden onder de Coronacrisis. Waarvan velen zich proberen te houden aan alle maatregelen in deze tijden. Dat er dan mensen zijn die over de rug van al deze mensen geld willen verdienen is ongehoord.”

Vanwege het lopende onderzoek kan de GGD GHOR Nederland momenteel geen uitspraken doen over de zaak. Wij verwachten dat deze criminele actie vragen oproept over de veiligheid van het laten testen en de manier waarop de GGD'en met de persoonsgegevens omgaan. Testen is een enorm belangrijke schakel in het bestrijden van het virus. Het belang van (blijven) komen bij klachten is groot. GGD GHOR Nederland wil daarom binnen de beperkingen van het onderzoek zo transparant mogelijk zijn over het incident en de gevolgen.

In de bijgaande pdf staan de vragen en antwoorden. Mogelijk worden deze gedurende dag en/of week verder aangevuld. Daarom vermelden we bovenaan het document het moment van de laatste wijzigingen.

Vragen en antwoorden (25-01-'21 15.00u)

Hoe is deze situatie bekend geraakt bij GGD GHOR Nederland?

Via een tip van een journalist van RTL afgelopen vrijdag.

Wat hebben jullie gedaan na de tip?

We hebben meteen contact opgenomen met de politie, aangifte gedaan en een melding gedaan bij de Autoriteit Persoonsgegevens. Vervolgens hebben wij controles uitgevoerd in onze systemen én volledige toegang gegeven aan de politie tot onze systemen om de opsporing zo goed mogelijk plaats te kunnen laten vinden.

Hoe controleren jullie zelf?

Wij controleren op verschillende manieren hoe onze medewerkers omgaan met de informatie in onze systemen. En dat heeft eerder geleid tot de ontdekking van onregelmatigheden en tot het nemen van maatregelen. Daarnaast beschermen we ons tegen aanvallen op onze systemen van buiten. Wij verwerken grote volumes gegevens, en deze actie is in onze controles niet naar voren gekomen.

Welke controlemechanismen hebben jullie om misbruik te voorkomen?

Dat zijn er verschillende:

1. We hebben controle aan de poort. Mensen moeten een VOG aanleveren en een geheimhoudingsverklaring ondertekenen. Daarmee is duidelijk dat ze aansprakelijk zijn op het moment dat zij zich niet aan de voorwaarden van de overeenkomst houden.
2. Daarnaast zijn privacy en geheimhouding doorlopend onderwerp van onze trainingen en gesprekken.
3. Wij controleren sinds de start het gebruik van onze systemen door de medewerkers, en hebben onze controles steeds verder verbeterd en doen dat nog steeds. Vanwege het belang van de virusbestrijding en de gevraagde snelheid zijn wij – op diverse manieren – met steekproefsgewijze controles van start gegaan. Over dit uitgangspunt zijn wij altijd transparant geweest. De Autoriteit Persoonsgegevens heeft tot nu toe geen aanvullende vragen gesteld over de werkwijze.
4. Alleen mensen die voor hun werk noodzakelijk toegang moeten hebben tot een persoonsdossier, mogen dit dossier inzien. Hierop controleren we zoals gezegd steekproefsgewijs. Bij verboden toegang volgt ontslag en indien nodig aangifte.
5. Daarnaast schalen we de monitoring van het gebruik van onze systemen verder op. We verwachten we eind maart systemen te implementeren die automatisch en continue zullen controleren. Hier werken wij al geruime tijd aan.

Om welke systemen gaat het?

Het gaat om CoronIT. Dit is het administratiesysteem voor het test- en vaccinatieproces en de communicatie hierover. Dus als je een afspraak maakt voor een coronatest via het callcenter, de coronatest website of een arts, komen je persoonsgegevens in CoronIT. Ook als je een afspraak maakt voor een vaccinatie.

Daarnaast lijkt er ook sprake te zijn van HPZone is een elektronisch dossier wat de GGD'en gebruiken om het bron- en contactonderzoek uit te voeren. Als iemand een positieve testuitslag heeft en deze gemeld wordt bij de GGD, dan wordt een dossier van deze persoon in HPZone aangemaakt.

Welke informatie leggen jullie van mensen vast

Wij leggen persoonsgegevens vast zoals naam, adres, woonplaats, telefoonnummer/e-mailadres, BSN, geslacht, geboortedatum. Daarnaast afhankelijk van het contact ook test- en/of vaccineerafspraken en testresultaten.

Is er sprake van een bron en contactonderzoek (in HPZone) dan wordt daarin ook de informatie uit de bron- en contactonderzoek gesprekken vastgelegd. Dit is onder andere: noodzakelijke medische gegevens (bijvoorbeeld klachten/symptomen en huisarts), waar iemand is geweest en met wie hij/zij in contact is geweest. Ook wordt informatie vastgelegd van bron(nen) en nauwe contacten. Deze informatie is beperkt.

Wat doen medewerkers in de systemen?

Medewerkers van het callcenter (inbound – die gebeld worden) kunnen via CoronIT testafspraken en vaccinatieafspraken maken. Verder kunnen de (outbound – die mensen bellen) callagents de testuitslagen zien, aangezien zij mensen, zonder DigiD, bellen met hun testuitslag. Bron- en contactonderzoekers leggen alle gegevens rondom een besmetting vast in HP-zone.

Welke gegevens van een persoon kunnen de medewerkers inzien

Dat hangt van de rol van de gebruiker af: De gebruiker ziet alleen die gegevens die hij of zij op dat moment voor zijn werk nodig heeft. Voor mensen die werken bij het call-centrum voor testafspraken zijn bijvoorbeeld de gezondheidsverklaringen die voor vaccinaties worden ingevuld niet zichtbaar. Registratie van bijwerkingen is alleen toegankelijk voor mensen met medische autorisatie.

Staan de gegevens van alle Nederlanders in jullie systemen?

Nee, in onze systemen staan alleen de gegevens van de mensen die de afgelopen tijd met de GGD te maken hebben gehad voor een testafpraak, bron- en contactonderzoek of een vaccinatie

Hebben evenveel mensen toegang tot mijn gegevens bij vaccineren?

De medische gegevens die bij vaccinaties worden vastgelegd zijn afgeschermd en niet zichtbaar voor medewerkers die zich met testen bezighouden. Omdat iedereen maar één dossier heeft en iedereen zich ook kan laten testen zijn persoonsgegevens wel in te zien.