Q&A RTL Nieuws CoronIT

versie 29 januari 08.00 u

Hier vindt u veelgestelde vragen en de antwoorden over de datadiefstal die recent heeft plaatsgevonden uit de systemen van de GGD. U kunt uw vraag vinden door te navigeren via de linkerkolom.

We kunnen ons voorstellen dat de datadiefstal vragen oproept en mogelijk uw vertrouwen in ons heeft geschaad. Dit vinden wij heel erg. We willen u zo goed mogelijk informeren en daarom vullen wij deze veelgestelde vragen steeds aan met nieuwe informatie.

Er loopt op dit moment een politieonderzoek, waardoor we nog niet precies weten hoe groot de datadiefstal is. Ook mogen we bepaalde details nog niet delen, omdat dit mogelijk het onderzoek in gevaar brengt.

Heeft u een vraag die hier niet bij staat? Bel dan met ons speciale nummer: 085-1308226 elke dag bereikbaar van 9:00u tot 21:00u

TOP 3 MEESTGESTELDE VRAGEN

1. **Wat is er precies gebeurd?**
   Er zijn persoonsgegevens gestolen door medewerkers van de GGD. Deze gegevens gaan over het testen op het COVID-19-virus en mogelijk het bron- en contactonderzoek en bevatten onder andere naam, adres, BSN, telefoonnummer, e-mailadres, testuitslag en testlocatie. Of de gegevens ook zijn verkocht en om wiens gegevens het gaat, maakt deel uit van het politieonderzoek. Meer informatie is te vinden op de site van de politie

2. **Zijn mijn gegevens gestolen?**
   Dat kunnen wij nu nog niet zeggen. Dit maakt onderdeel uit van het politieonderzoek. Op het moment dat vast komt te staan dat uw gegevens gestolen zijn, dan informeren wij u daar over.

3. **Wat zijn de mogelijke gevolgen? Welk risico loop ik als criminelen mijn persoonsgegevens hebben? En waarop moet ik letten?**

- U loopt het risico slachtoffer te worden van oplichting. Criminelen bellen of mailen u bijvoorbeeld uit naam van een voor u geloofwaardige instantie zoals uw bank. Ze zouden uw vertrouwen kunnen winnen, omdat ze persoonlijke informatie noemen (zoals uw geboortedatum of woonadres). Voordat u het weet, heeft u een betaling voor iets gedaan – maar feitelijk op een phishinglink geklikt. Ontdek hier hoe u zich kunt beschermen tegen phishing.

- Een ander risico is identiteitsfraude. De fraudeur gebruikt uw persoonsgegevens bijvoorbeeld om producten en diensten te krijgen op uw naam. Of om een bankrekening te openen of een creditcard aan te vragen. Ontdek hier meer informatie over identiteitsfraude.
- Activeer tweestapsverificatie op uw social media accounts, e-mail. Een overzichtelijke manier hoe u dit kunt inschakelen treft u hier aan.
- Maakt u gebruik van WhatsApp? Criminelen maken steeds vaker gebruik van de 'vriend in nood fraude'. Ons advies is om hier ook een extra beveiliging in te stellen. Hoe u dat doet leest u hier.

Doe altijd aangifte als u slachtoffer wordt van cybercrime.

OVER DE DATADIEFSTAL

4. **Hoe is GGD GHOR Nederland er achter gekomen dat er werd gehandeld in privégegevens afkomstig uit CoronIT**
   Naar aanleiding van vragen die ons zijn gesteld door een journalist van RTL nieuws.

5. **Wat is er precies gebeurd?**
   Er zijn persoonsgegevens gestolen. Deze gegevens gaan over het testen op het COVID-19-virus en mogelijk het bron- en contactonderzoek en bevatten onder andere naam, adres, BSN, testuitslag en testlocatie. Of de gegevens ook zijn verkocht en om wiens gegevens het gaat, maakt deel uit van het politieonderzoek. Meer informatie is te vinden op de site van de politie.

6. **Hadden jullie dit zelf niet moeten ontdekken?**
   Wij controleren op verschillende manieren hoe onze medewerkers omgaan met de informatie in onze systemen. En dat leidt tot de ontdekking van onregelmatigheden en tot het nemen van maatregelen. Daarnaast beschermen we ons tegen aanvallen op onze systemen van buitenaf. Deze diefstal is in onze controles niet naar voren gekomen.

7. **Wat hebben jullie gedaan na deze vragen?**
   We hebben meteen onderzoek ingesteld. Vervolgens contact opgenomen met de politie, aangifte gedaan en een melding gedaan bij de Autoriteit Persoonsgegevens. Vervolgens hebben wij zelf controles uitgevoerd in onze systemen én volledige toegang verstrekt aan de politie om de opsporing zo goed mogelijk plaats te kunnen laten vinden.

8. **Welke privégegevens worden via welk medium/platform aangeboden?**
   Hierover kunnen wij voor nu geen uitspraken doen, dit is onderdeel van het onderzoek van politie en justitie.

9. **Van hoeveel mensen zijn privégegevens verkocht? In welke periode?**

Hierover kunnen wij voor nu geen uitspraken doen, dit is onderdeel van het onderzoek van politie en justitie.

10. Hoeveel GGD-medewerkers hebben in deze privégegevens gehandeld?

Hierover kunnen wij voor nu geen uitspraken doen, dit is onderdeel van het onderzoek van politie en openbaar ministerie.

11. Welke actie is genomen richting de betreffende medewerkers?

Er zijn in ieder geval twee medewerkers gearresteerd. Maar onderzoek van politie en justitie loopt. Zij zullen hierover communiceren zodra ze dat kunnen.

SYSTEMEN

12. Uit welke systemen is er sprake geweest van datadiefstal?

Het gaat om CoronIT. Dit is het administratiesysteem voor het testen en vaccineren en de communicatie hierover. Dus wanneer u een afspraak maakt voor een COVID-19-test via het callcenter, de COVID-19-test website of een arts, komen uw persoonsgegevens in CoronIT. Ook wanneer u een afspraak maakt voor een vaccinatie.

Daarnaast lijkt er ook sprake te zijn van diefstal van persoonsgegevens uit HPZone. We hebben vernomen dat gestolen persoonsgegevens worden aangeboden, maar hebben nog niet kunnen vaststellen dat ze feitelijk verhandeld zijn. Dat is onderwerp van het onderzoek dat de politie nu doet.

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.

13. Zijn mijn gegevens wel veilig bij jullie?

Geen enkel IT-systeem is onfeilbaar. De GGD doet alles wat in haar vermogen ligt om ervoor te zorgen dat gegevens van mensen die zich laten testen in veilige handen zijn. Daarom hebben we ook na dit incident maatregelen genomen. Om dit soort incidenten in de toekomst te voorkomen. Maar helaas kunnen we dit niet 100% uitsluiten. Hoe wij ervoor zorgen dat uw gegevens zo veilig mogelijk zijn, leest u hier (link naar ander antwoord.).

14. Zijn de systemen voor testen, bron- en contact onderzoek en vaccineren strikt gescheiden?

Gegevens van testen en vaccineren bevinden zich in CoronIT. De medische gegevens die bij vaccinaties worden vastgelegd zijn afgeschermd en niet zichtbaar voor medewerkers die zich

met testen bezighouden. Wel is er een koppeling waardoor een testuitslag altijd te zien is, wanneer iemand in het systeem kijkt bij een vaccinatie afspraak. Dit is zo ingericht omdat het nodig kan zijn om te bepalen of iemand gevaccineerd kan worden.

De gegevens van het Bron- en contactonderzoek bevinden zich in HPZone.,

15. **Hoeveel Nederlanders staan er in CoronIT en HPzone?**
    In CoronIT staan gegevens van circa ca. 5,5 miljoen mensen. In HPZone van circa 1 miljoen

16. **Hoeveel medewerkers hebben toegang tot CoronIT**
    In totaal gaat dit om ca. 26.000 medewerkers. Zowel bij de GGD'en als bij bedrijven die gecontracteerd zijn voor de COVID-19-bestrijding.

17. **Wat doen de medewerkers in CoronIT en HPZone?**

    Medewerkers van het callcenter die telefoontjes ontvangen kunnen via CoronIT testafspraken en vaccinatieafspraken maken. Verder kunnen de medewerkers die uitgaande telefoontjes plegen de testuitslagen zien, zodat ze die kunnen meedelen.

    Bron- en contactonderzoekers leggen alle gegevens rondom een besmetting vast in HPZone.

CORONIT

18. **Wat is er precies gestolen uit Coronit**
    CoronIT is het administratiesysteem voor het test- en vaccinatieproces. Het gaat daarbij om de persoonsgegevens van losse personen. Niet om het downloaden van complete datasets. Er zijn twee verdachten gearresteerd op verdenking van het te koop aanbieden van persoonsgegevens uit de systemen die de GGD gebruikt voor de COVID-19 testen.

19. **Is het normaal dat zoveel medewerkers toegang hebben tot deze gegevens? En waarom is dit nodig?**
    De GGD'en willen het COVID-19-virus zo goed mogelijk bestrijden. Daarbij zijn zeer veel medewerkers betrokken. Elke callcenter medewerker die telefoontjes aanneemt (inbound) moet afspraken kunnen maken. En iedere callcenter medewerker die mensen belt (outbound) moet uitslagen door kunnen gegeven als deze binnen zijn.

20. **Wat doen we aan extra controles in CoronIT**

We verbeteren onze systemen continue. Aan de hand van dit incident hebben we wederom verdere aanscherpingen gedaan. We maken de mogelijkheden om te zoeken naar mensen in de systemen veel beperkter door de zoekfunctie aan te passen. De zoekacties die gedaan worden,

worden gelogd. FOX IT doet op dit moment forensisch onderzoek naar onze logging (de handelingen die in het systeem verricht zijn). En tot de lancering van vol-automatisch en continu controleren eind maart, blijft FOX IT voor ons de loggings controleren. Zo proberen we verdacht gedrag te ontdekken. Bovendien hebben we een team dat 7 dagen per week handmatig verdachte handelingen opspoort.

21. Wat betekent het beperken van de toegang voor de toegankelijkheid van testen en bron- en contactonderzoek

Beperkingen in toegang van mensen tot gegevens vertraagt de snelheid waarmee wij ons werk kunnen doen en verlengt de doorlooptijden. Bijvoorbeeld de snelheid waarmee we testuitslagen kunnen doorgeven en testafspraken kunnen maken.

HPZONE

22. Waarom werken jullie (nog) met HPZone?

HPZone was het enige systeem dat voorhanden was om in maart 2020 in vliegende vaart aan de slag te gaan. We hebben aan het begin geconstateerd dat HPZone niet aan de eisen van deze tijd voldoet, hebben aanpassingen gepleegd, maar wisten ook dat een nieuw systeem nodig was.

We waren al bezig om over te gaan naar een nieuw, beter systeem. Dat zal versneld gaan gebeuren. Het exacte moment dat we overgaan kunnen wij nog niet noemen.

23. Wie heeft er allemaal toegang tot HPZone

In HPZone hebben de eigen GGD-artsen en verpleegkundigen toegang en alle (tijdelijke) medewerkers die bron- en contactonderzoek doen.

24. Klopt het dat er datasets uit HPZone zijn aangeboden?

We hebben vernomen dat datasets worden aangeboden, maar hebben nog niet kunnen vaststellen dat ze feitelijk verhandeld zijn. Dat is onderwerp van het onderzoek dat de politie nu doet.

25. Hoe kan het dat er sprake is van het exporteren van een dataset

In CoronIT kan dit niet. In HP Zone kon dit wel.

Om een goed beeld te hebben van de COVID-19 crisis maken GGD-epidemiologen rapportages op basis van datasets. De meeste daarvan zijn anoniem en bevatten alleen aantallen. Daarnaast krijgen GGD'en als zij dat willen exports van de gegevens van mensen die in hun GGD-regio getest of gevaccineerd zijn, zodat zij die kunnen gebruiken voor het

maken van rapporten voor bijvoorbeeld de gemeenten. De rechten worden beheerd door de GGD'en en de exports worden gelogd.

26. Klopt het dat die functie nu is uitgezet?

Ja, de belangrijkste export mogelijkheden hebben we uitgezet. We werken ook aan het aanpassen van alle overige exportmogelijkheden. De rechten voor gebruik van de resterende, benodigde exportfunctionaliteit zijn aan minder mensen toegekend op basis van beperktere rollen.

27. Wat betekent het afsluiten van deze export functie voor het werk van BCO-mensen

Onder andere de werkverdeling is per direct lastiger geworden.

28. HP Zone en HP Zone Lite. Wat is het verschil

HP Zone Lite is een variant van HPzone waarmee alleen COVID19 data beschikbaar wordt gesteld aan gebruikers.

29. Waarom hebben jullie HPZone Lite geïmplementeerd (in augustus)

HPZone Lite is bedoeld om grote aantallen medewerkers makkelijk te laten werken aan bron- en contactonderzoek. In de eerste golf liepen GGD regio's over en konden andere GGD regio's hen niet helpen. Dat hebben we opgelost in HPZone Lite, door het systeem zo in te richten dat GGD'en elkaar wel konden helpen. hierdoor konden veel meer bron- en contactonderzoeker hun werk doen.

30. Kan een medewerker van GGD-regio Groningen in een bron-en contactonderzoek casus van GGD regio Utrecht?

Nee, in principe niet. Soms blijven bron- en contactmedewerkers toegang houden tot gegevens van GGD-regio's, waar ze eerder voor gewerkt hebben. Zodat ze snel weer kunnen inspringen als dit nodig is voor virusbestrijding.

31. Wat gaan jullie doen om de tijd tot de introductie van het nieuwe systeem wel veilig te overbruggen?

GGD GHOR Nederland heeft een gespecialiseerd bureau opdracht gegeven tot het in kaart brengen en realiseren van alle noodzakelijke wijzingen om het systeem te laten voldoen aan veiligheidseisen

PERSOONLIJKE GEGEVENS

32. Welke informatie van mensen staat in Coronit en HP Zone

In CoronIT staan onder andere naam, adres, woonplaats, telefoonnummer/e-mailadres, BSN, geslacht, geboortedatum, test- en/of vaccineerafspraken en testresultaten. Contra-indicaties en COVID-19 klachten.

In HPZone staan naam, adres, woonplaats, telefoonnummer, geslacht, geboortedatum en BSN van een persoon. Verder wordt in HPZone 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.

De gegevens zoals geregistreerd in CoronIT zijn opgenomen in de privacyverklaring CoronIT. Hetzelfde geldt voor HPZone, deze zijn terug te vinden in de privacyverklaring van bron- en contactonderzoek in het kader van COVID-19.

33. Waarom zijn mijn volledige persoonsgegevens en BSN nodig voor het maken van een testafspraak?

Volledige persoonsgegevens zijn nodig, zodat wij zeker weten dat wij een test of vaccinatie afspraak maken met de juiste persoon.

Het BSN is belangrijk, zodat in ons systeem automatisch de juiste persoonsgegevens geregistreerd worden in plaats van dat alle persoonsgegevens handmatig ingevoerd moeten worden (met het risico op administratieve fouten). Daarnaast is het BSN gekoppeld aan DigiD, wat het mogelijk maakt om de uitslag online in te zien. Het woonadres is nodig, zodat we de uitslag ook per brief kunnen toesturen indien er onverhoopt een verkeerd telefoonnummer is geregistreerd en daardoor iemand de uitslag niet heeft kunnen ontvangen.

34. 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 callcenter dat testafspraken maakt zijn bijvoorbeeld de gezondheidsverklaringen die voor vaccinaties worden ingevuld niet zichtbaar. Registratie van bijwerkingen is alleen toegankelijk voor mensen met medische autorisatie.

35. Staan de gegevens van alle Nederlanders in CoronIT en HPZone?

Nee, in CoronIT staan alleen de gegevens van personen die een test of vaccinatie afspraak bij de GGD hebben gemaakt.

In HPZone staan alleen de gegevens van de personen die een positieve COVID-19 test hebben ontvangen en van mensen die als huisgenoot of als nauw contact uit bron- en contactonderzoek kwamen.

BEVEILIGING

36. Welke controle mechanismen hebben jullie om datadiefstal te voorkomen in Coronit en HP Zone?

Dat zijn er verschillende:

- Mensen moeten een Verklaring Omtrent het Gedrag (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
- Privacy en geheimhouding zijn een doorlopend onderwerp van onze trainingen en tijdens gesprekken.
- Wij controleren het gebruik van onze systemen door de medewerkers, en hebben onze controles steeds verder verbeterd. Vanwege het belang van de virusbestrijding en de gevraagde snelheid zijn wij – op diverse manieren – met steekproefsgewijze controles van start gegaan. Specifiek over Coronit heeft de Autoriteit Persoonsgegevens ons in oktober vragen gesteld. Deze hebben wij beantwoord, waarna er tot een paar dagen geleden geen aanvullende vragen zijn gesteld over de werkwijze. De manier waarop wij in Coronit en HPZone controleren verschilt. Dat komt door de technische mogelijkheden
- Alleen mensen die voor hun werk inzage moeten hebben in een persoonsdossier voor hun werk, mogen dit dossier inzien. Hierop controleren we zoals gezegd steekproefsgewijs. Bij niet voor het werk noodzakelijke inzage volgt ontslag en indien nodig aangifte. Enkele tientallen mensen zijn om die reden ontslagen.
- We verwachten we eind maart systemen te implementeren die automatisch en continue niet-noodzakelijke toegang controleren. Om zo verdacht gedrag op te sporen

37. Hoe gaat de GGD voorkomen dat de illegale handel van gegevens uit CoronIT en HPzone in de toekomst kan plaatsvinden?

We werken intensief samen met de politie om daders op te sporen en er voor te zorgen dat gegevens niet verder gedeeld kunnen worden. Daarnaast zijn we continu bezig om onze werkprocessen te verbeteren en de veiligheid van onze systemen te vergroten. Welke maatregelen we precies nemen kunnen we, omwille van de veiligheid, niet toelichten. Anders dan de maatregelen die we reeds noemen bij vraag [invullen]

TESTEN

38. Kan ik me nog wel veilig laten testen?

Ja, het is belangrijk dat u zich laat testen, vaccineren en deelneemt aan bron- en contactonderzoek. De datadiefstal gaat om incidenten, waarbij we alles op alles zetten om daders aan te geven en voorzorgsmaatregelen te treffen. We zijn continu bezig om onze werkprocessen te verbeteren en de veiligheid van onze systemen te vergroten.

39. Ik heb een COVID-19 test gedaan bij een andere organisatie dan de GGD. Staan mijn gegevens nu ook in jullie systemen?

Als uw testuitslag negatief is niet. Als u een positieve testuitslag had, dan worden uw gegevens in HPZone opgenomen. Alleen positieve uitslagen zijn andere organisaties verplicht aan ons te melden.

40. Ik heb een test gedaan en was negatief. Sta ik dan ook in het systeem?

Als u zich bij de GGD heeft laten testen en de uitslag was negatief dan staat u in CoronIT. Als u zich bij een andere partij heeft laten testen en uw uitslag was negatief dan staat u niet in onze systemen.

VACCINEREN

41. Kan ik me nog wel veilig laten vaccineren?

Ja, het is belangrijk dat u zich laat testen, vaccineren en deelneemt aan bron- en contactonderzoek. De datadiefstal gaat om incidenten, waarbij we alles op alles zetten om daders aan te geven en voorzorgsmaatregelen te treffen. We zijn continu bezig om onze werkprocessen te verbeteren en de veiligheid van onze systemen te vergroten.

42. Hebben evenveel mensen toegang tot mijn gegevens bij vaccineren als bij de COVID19-testen?

Gegevens van zowel testen en vaccineren bevinden zich in CoronIT. De medische gegevens die bij vaccinaties worden vastgelegd zijn afgeschermd en niet zichtbaar voor medewerkers die zich met testen bezighouden. Wel is er een koppeling waardoor een testuitslag altijd te zien is, wanneer iemand in het systeem kijkt bij een vaccinatie afspraak. Omdat dat nodig kan zijn om te bepalen of u gevaccineerd kunt worden

HOE HELPEN WIJ U

43. Wat doet u om te voorkomen dat mensen van wie nu de gegevens in omloop kunnen zijn, geen slachtoffer worden van fraude

We werken intensief samen met de politie om daders op te sporen en er voor te zorgen dat gegevens niet verder gedeeld kunnen worden. Verder proberen we op deze pagina tips te geven hoe men zich kan wapenen tegen cybercriminelen. [link naar 49]

Op het moment dat vast komt te staan dat uw gegevens gestolen zijn, dan zullen wij u hierover informeren.

44. Kunnen jullie controleren of mijn gegevens gestolen zijn bij de datadiefstal?

Nee, dat kunnen wij op dit moment niet. De politie doet namelijk nog onderzoek naar welke

gegevens gestolen zijn. Het is nu nog onduidelijk welke data er gestolen zijn en om wiens gegevens het gaat. Het is onze plicht om mensen te informeren als hun gegevens betrokken zijn bij datadiefstal. Maar daar valt nu helaas nog niets over te zeggen.

45. Kunnen mijn gegevens ook verwijderd worden uit jullie systemen nadat ik getest ben / er bron- en contact onderzoek heeft plaatsgevonden ?

U heeft het recht om een verzoek te doen tot verwijdering of anonimisering van uw gegevens. Let wel, met het anonimiseren of verwijderen van uw gegevens is het voor de GGD minder goed mogelijk om de verspreiding van het virus te monitoren of tegen te gaan.

Wilt u dit toch, dan is hier een procedure voor via uw regionale GGD. U kunt hiervoor contact opnemen met uw regionale GGD. U vindt deze contactgegevens op www.ggd.nl.

46. Ik wil een klacht indienen over de manier waarop jullie met mijn persoonsgegevens omgaan

Dat kan. U kunt zich wenden tot onze functionaris gegevensbescherming via fg@ggdghor.nl.

47. Krijg ik een vergoeding als blijkt dat mijn data bij de datadiefstel zijn betrokken?

Daarover kunnen we nu nog niets zeggen. De politie doet op dit moment namelijk nog onderzoek naar de datadiefstal. Als het daadwerkelijk zou gaan om uw gegevens, wordt u hierover geïnformeerd.

48. Welk risico loop ik als criminelen mijn persoonsgegevens hebben? En waarop moet ik letten?

De website van de politie beschrijft de mogelijke gevolgen goed:

- U loopt het risico slachtoffer te worden van oplichting. Criminelen bellen of mailen u bijvoorbeeld uit naam van een voor u geloofwaardige instantie zoals uw bank. Ze zouden uw vertrouwen kunnen winnen, omdat ze persoonlijke informatie noemen (zoals uw geboortedatum of woonadres). Voordat u het weet, heeft u een betaling voor iets gedaan – maar feitelijk op een phishinglink geklikt. Ontdek hier hoe u zich kunt beschermen tegen phishing.
- Een ander risico is identiteitsfraude. De fraudeur gebruikt uw persoonsgegevens bijvoorbeeld om producten en diensten te krijgen op uw naam. Of om een bankrekening te openen of een creditcard aan te vragen. Ontdek hier meer informatie over identiteitsfraude.
- Activeer tweestapsverificatie op uw social media accounts, e-mail. Een overzichtelijke manier hoe u dit kunt inschakelen treft u hier aan.

- Maakt u gebruik van WhatsApp? Criminelen maken steeds vaker gebruik van de 'vriend in nood fraude'. Ons advies is om hier ook een extra beveiliging in te stellen. Hoe u dat doet leest u hier.

Doe altijd aangifte als u slachtoffer wordt van cybercrime.

49. Ik ben onlangs slachtoffer geworden van phishing/cybercrime. Kan dit komen doordat de GGD mijn gegevens had? En wat moet ik doen?

Als u slachtoffer bent van phishing/cybercrime, doe dan altijd aangifte op het politiebureau. De politie doet op dit moment namelijk nog onderzoek naar welke gegevens gestolen zijn bij de GGD. Het is nu nog onduidelijk welke data er gestolen zijn en om wiens gegevens het gaat.

50. Wat kan ik doen als ik zie dat iemand online of via een chatdienst persoonsgegevens verkoopt?

Bel direct de politie op 0900 8844. Of anoniem op 0800 7000. Melding doen, heeft altijd zin. Hiermee voorkomt u slachtoffers en kan de politie direct verdachten opsporen en hun criminele praktijken stoppen.

ONZE MEDEWERKERS

51. Klopt het dat u uw medewerkers verbiedt om te spreken met de pers of onder druk zet om dit niet te doen?

Nee, dit klopt niet. Wij staan alle pers te woord. Daarbij vragen wij onze medewerkers om in geval van persvragen contact op te nemen met onze persvoorlichters.

52. Klopt het dat u medewerkers boetes oplegt als ze naar buiten treden over hun werk?

Nee, dit klopt niet. Wel is het zo dat al onze medewerkers een geheimhoudingsverklaring ondertekenen. Dat doen we omdat onze medewerkers met gevoelige informatie zoals persoonsgegevens omgaan

CONTACT

Met wie kan ik contact opnemen voor vragen en klachten?

Heeft u vragen dan adviseren wij u om deze lijst met veelgestelde vragen goed door te nemen. Zit het antwoord op uw vraag er niet bij, neemt u dan contact op met het speciale nummer voor deze datadiefstal: 085-1308226 elke dag bereikbaar van 9:00u tot 21:00u