solv.
Anne Frankstraat 121
1018 BZ Amsterdam
T +31 (0)20 530 01 60
F +31 (0)20 530 01 70
www.solv.nl

Aangetekend
De Staat der Nederlanden (ministerie van Volksgezondheid, Welzijn en Sport)
T.a.v. Zijne Excellentie de minister van Volksgezondheid, Welzijn en Sport
Parnassusplein 5
2511 VX DEN HAAG

Alsmede per e-mail: minister@minvws.nl

Datum	8 februari 2022	Van	Douwe Linders, advocaat - linders@solv.nl
Onze ref.	Stichting ICAM c.s. / Staat c.s. (12843)		Yentl van den Winkel, advocaat - winkel@solv.nl
Uw ref.	-		Lora Mourcous, advocaat - mourcous@solv.nl

Betreft: Stichting ICAM c.s. / de Staat c.s.: aansprakelijkstelling, sommatie en uitnodiging tot overleg uit hoofde van artikel 3:305a BW betreffende het GGD-datalek

Excellentie,

Namens onze cliënten, de Stichting Initiatieven Collectieve Acties Massaschade te Amsterdam ("**Stichting ICAM**"), mevrouw [redacted], woonachtig te [redacted], de heer [redacted], woonachtig te [redacted], de heer [redacted], woonachtig te [redacted], mevrouw [redacted], woonachtig te [redacted], mevrouw [redacted], woonachtig te [redacted] en de heer [redacted], woonachtig te [redacted] (cliënten hierna gezamenlijk te noemen: "**Stichting ICAM c.s.**"), vragen wij uw aandacht voor onderstaande aansprakelijkstelling, sommatie en uitnodiging tot overleg in verband met het GGD-datalek.

Vooraf merken wij op dat Stichting ICAM c.s. meent dat de Staat (het ministerie van VWS) verantwoordelijk is voor het GGD-datalek en dat de Staat aansprakelijk is voor de daardoor veroorzaakte schade. Wij zullen dat in deze brief toelichten. Brieven van gelijke strekking sturen wij echter gelijktijdig ook aan onder andere de GGD'en (zie hoofdstuk 3). De reden daarvoor is gelegen in de omstandigheid dat uw voorganger – onder andere in antwoord op schriftelijke Kamervragen - expliciet heeft aangegeven dat hij van mening was dat niet de Staat, maar de GGD'en en koepelorganisatie GGD GHOR verantwoordelijk zijn voor het datalek.

Stichting ICAM c.s. zou bij voorkeur de GGD'en niet betrekken in deze zaak. Helaas noopt de hiervoor genoemde stellingname Stichting ICAM c.s. ertoe om ook de GGD'en en andere organisaties aan te schrijven. Zij treedt echter graag met u in overleg over de mogelijkheden om de GGD'en niet te hoeven aanspreken.

De Staat en de overige aangeschreven partijen (zie hoofdstuk 3) worden in deze brief verder ook wel gezamenlijk aangeduid als de "**Staat c.s.**"

1 AANLEIDING

1. Op 25 januari 2021 berichtte RTL Nieuws over een groot datalek bij de Gemeentelijke Gezondheidsdiensten ("**GGD'en**"). Uit onderzoek van RTL Nieuws bleek dat persoonsgegevens in de softwaresystemen die de GGD'en gebruiken bij het plannen van test- en vaccinatieafspraken en het uitvoeren van bron- en contactonderzoek (CoronIT, HPZone en HPZone Lite) toegankelijk waren voor onbevoegden, online te koop werden aangeboden en waarschijnlijk werden verkocht aan internetcriminelen. De persoonsgegevens van in ieder geval 6,5 miljoen mensen, waaronder BSN's en gezondheidsgegevens, waren toegankelijk en beschikbaar voor illegale datahandel. Vastgesteld is dat van ten minste 1.250 mensen de persoonsgegevens daadwerkelijk zijn gestolen en waarschijnlijk verkocht. Inmiddels is bekend dat het werkelijke aantal waarschijnlijk veel groter is.[1]

2. Zoals door uw voorganger en GGD GHOR-voorzitter de heer Rouvoet is erkend,[2] was sprake van een grootschalig en ernstig datalek, met grote risico's voor alle 6,5 miljoen betrokken burgers. Persoonsgegevens waren zonder noodzaak toegankelijk voor een zeer groot aantal personen. Deze personen konden zonder adequate controle en beveiliging inloggen op de systemen en zonder beperkingen hun inloggegevens delen met derden. Zij hadden de mogelijkheid persoonsgegevens in bulk te downloaden en/of te printen, terwijl zij geen (goede) training en uitleg hadden gehad over privacy en gegevensbescherming. Er was daarnaast geen adequate controle op de betrouwbaarheid van deze personen en hun activiteiten in de softwaresystemen werden ontoereikend gemonitord en gelogd.

3. Het voorgaande is bevestigd door de Autoriteit Persoonsgegevens ("**AP**"), die naar aanleiding van het datalek een onderzoek heeft ingesteld naar de beveiliging van de softwaresystemen. In het onderzoek van de AP, waarover op 8 november jl. een indringende brief is gestuurd naar GGD GHOR en de GGD'en, is ook vastgesteld dat er na het datalek weliswaar maatregelen zijn getroffen, maar dat de beveiliging op dat moment nog steeds onvoldoende was. Volgens de AP bestonden er nog steeds "*wezenlijke risico's voor de bescherming van persoonsgegevens bij het testen,*

---

1 https://www.rtlnieuws.nl/nieuws/nederland/artikel/5247728/datalek-datadiefstal-ggd-gedupeerden.

2 Zie onder andere *Kamerstukken II* 2020-2021, 27 529, nr. 235, Verslag Schriftelijk Overleg (VSO) inzake datalek bij de coronasystemen van de GGD en 'GGD wist al maanden van privacyproblemen' en https://www.rtlnieuws.nl/nieuws/nederland/artikel/5211580/rouvoet-ggd-datalek-gegevens-gestolen-onderzoek-privacy.

vaccineren en het bron- en contactonderzoek tijdens de coronapandemie."[3] Dat de beveiliging van de softwaresystemen nog steeds niet adequaat is, werd duidelijk op 3 februari jl.[4]

4. Het GGD-datalek is niet het eerste incident waarbij is gebleken dat de overheid (de beveiliging van) haar IT-systemen niet op orde heeft, onvoldoende aandacht heeft voor de bescherming van persoonsgegevens en laks omgaat met de privacy van burgers. Voorbeelden daarvan zijn de toeslagenaffaire, de UWV-datalekken,[5] het Donorregister-datalek[6] en het Infectieradar-datalek.[7] Net als in die gevallen zijn ook deze keer de meest elementaire basismaatregelen van IT-beveiliging niet (voldoende) in acht genomen, ondanks dat het ministerie van VWS en de GGD'en meerdere keren zijn gewaarschuwd. Dat is ernstig verwijtbaar, zeker nu het gaat om zeer gevoelige persoonsgegevens van miljoenen mensen. Terwijl de overheid stringente privacyregelgeving heeft ingevoerd en handhaaft, en substantiële boetes oplegt als die normen onvoldoende worden nageleefd, blijkt keer op keer dat diezelfde overheid de regels niét naleeft en dienaangaande niet of nauwelijks wordt beboet of tot vergoeding van schade overgaat.

5. Het GGD-datalek heeft de privacy van burgers ernstig in gevaar gebracht. Minimaal 6,5 miljoen mensen lopen momenteel het risico slachtoffer te worden van identiteitsfraude en oplichting. Voor een deel van die mensen is dat risico al verwezenlijkt.

6. Naast die risico's en de (daardoor) veroorzaakte schade, creëert dit soort incidenten het risico dat burgers het vertrouwen in de overheid kwijtraken. Dat is vanzelfsprekend hoogst ongewenst, zeker in een crisis als de coronapandemie. Dat risico wordt vergroot door de welhaast laconieke reacties die veelal volgen op dergelijke incidenten: er worden excuses aangeboden in de Kamer, één van de grote consultancykantoren wordt gevraagd om een auditrapport op te stellen en iedereen spreekt zijn ontsteltenis uit over de bevindingen, maar tot wezenlijke veranderingen ter voorkoming van herhaling komt het niet. De overheid neemt geen of onvoldoende verantwoordelijkheid en doet weinig moeite om die indruk bij burgers weg te nemen.

7. Stichting ICAM c.s. meent dat het in het belang is van alle burgers en ondernemingen in Nederland dat dit verandert. De Staat is het aan hen verplicht om zowel preventief als na een incident op een serieuze wijze verantwoordelijkheid te nemen voor IT-beveiliging en de bescherming van persoonsgegevens, een taak die in de huidige informatiesamenleving steeds belangrijker wordt. Onderdeel daarvan is ook dat de Staat inzake het GGD-datalek adequate inspanningen levert om

---

3 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ggd-moet-persoonsgegevens-beter-beschermen.

4 https://www.gelderlander.nl/home/ggd-laks-met-beschermen-privacy-oud-medewerker-kan-vanuit-huis-bij-jouw-gegevens~a922a62b/ en https://www.vpngids.nl/nieuws/ggd-heeft-privacyzaakjes-nog-altijd-niet-op-orde/.

5 https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/uwv-krijgt-boete-voor-slechte-beveiliging-bij-verzending-groepsberichten.

6 https://zoek.officielebekendmakingen.nl/kst-32761-160.html#ID-926322-d36e82.

7 https://zoek.officielebekendmakingen.nl/ah-tk-20192020-3564.html en https://zoek.officielebekendmakingen.nl/ah-tk-20192020-3563.html.

te achterhalen hoe groot het GGD-datalek werkelijk is en welke schade er precies voor welk deel van de burgers is ontstaan. Ook dient ze de gedupeerde burgers schadeloos te stellen.

8. In deze brief stelt Stichting ICAM de Staat c.s. primair namens alle gedupeerden van het GGD-datalek aansprakelijk voor de geleden schade, dit op de voet van artikel 3:305a BW, en subsidiair namens de bij Stichting ICAM aangesloten deelnemers, dit op de voet van met hen gesloten overeenkomsten van opdracht. De individuele gedupeerden genoemd in hoofdstuk 2 stellen de Staat c.s. hierbij zelf aansprakelijk voor de door hen geleden schade. Daarnaast sommeert Stichting ICAM c.s. de Staat c.s. om adequate maatregelen te nemen, om te voorkomen dat dit type incidenten zich in de toekomst opnieuw zal voordoen.

9. Voorts is deze brief bedoeld als uitnodiging om in overleg te treden om te verkennen of een oplossing buiten rechte kan worden bereikt, zoals vereist op grond van artikel 3:305a lid 3 sub (c) van het Burgerlijk Wetboek ("**BW**").

2 STICHTING ICAM EN DE INDIVIDUELE GEDUPEERDEN

10. Stichting ICAM is een belangenorganisatie zonder winstoogmerk die opkomt voor de belangen van groepen gedupeerden zoals bedoeld in artikel 3:305a BW. Zij treedt in het bijzonder op tegen inbreuken op de persoonlijke levenssfeer en de bescherming van persoonsgegevens, en uitdrukkelijk tegen dergelijke inbreuken door de overheid. De statuten van Stichting ICAM zijn als **Bijlage 1** bij deze brief gevoegd.

11. Stichting ICAM behartigt de belangen van alle gedupeerden van het GGD-datalek. Zij doet dat op grond van artikel 3:305a BW. Stichting ICAM voldoet aan alle vereisten die in dat artikel en in de artikelen 1018a e.v. van het Wetboek van Burgerlijke rechtsvordering ("**Rv**") worden gesteld. Als 3:305a-belangenorganisatie heeft Stichting ICAM ook op grond van artikel 79, 80 en 82 van de Algemene Verordening Gegevensbescherming ("**AVG**") het recht om de gedupeerden te vertegenwoordigen. Bovendien heeft Stichting ICAM ten tijde van het versturen van deze brief van reeds bijna 80.000 mensen een contractueel mandaat gekregen om hen te vertegenwoordigen jegens de Staat c.s. en namens hen bepaalde rechten en bevoegdheden uit te oefenen, zoals vermeld in de deelnemersovereenkomst die zij met deze deelnemers heeft gesloten (**Bijlage 2**). Meer informatie over Stichting ICAM kunt u vinden op de website https://www.datalek-ggd.nl/.

12. Mevrouw [redacted] ontving op 18 maart 2021 een brief van GGD GHOR. In die brief meldt GGD GHOR dat mevrouw [redacted] één van de personen is van wie gegevens onbevoegd zijn ingezien, gestolen en waarschijnlijk verkocht. Mevrouw [redacted] is aldus één van de gedupeerden in de groep van (momenteel) 1.250 mensen van wie vaststaat dat hun persoonsgegevens zijn ontvreemd. Opmerkelijk is dat mevrouw [redacted] zich op het moment van ontvangen van de brief nog nooit had laten testen of vaccineren en voor zover zij weet – ook geen

onderdeel was geweest van bron- en contactonderzoek. Op welke wijze haar gegevens in de GGD-systemen terecht zijn gekomen is aldus onduidelijk. Mevrouw [redacted] heeft lange tijd een onveilig gevoel overgehouden aan het feit dat haar persoonsgegevens zijn ontvreemd. Zo heeft zij gedurende enkele maanden stelselmatig haar bankafschriften gecontroleerd.

13. De heer [redacted] ontving op 19 maart 2021 dezelfde brief als mevrouw [redacted] en is dus eveneens één van de gedupeerden in de groep van (momenteel) 1.250 mensen van wie vaststaat dat hun persoonsgegevens zijn ontvreemd. Hij heeft zich op 25 januari 2021 voor het eerst laten testen.

14. Ook de heer [redacted] ontving een brief van GGD GHOR waaruit blijkt dat zijn gegevens onbevoegd zijn ingezien, gestolen en waarschijnlijk verkocht. Ook hij is dus één van de gedupeerden in de groep van (momenteel) 1.250 mensen van wie vaststaat dat hun persoonsgegevens zijn ontvreemd. De heer [redacted] is onderdeel geweest van bron- en contactonderzoek en heeft zich laten vaccineren. Hij wordt sindsdien regelmatig lastiggevallen door telefoontjes van onbekende nummers. De heer [redacted] heeft sterk het vermoeden dat dit samenhangt met het GGD-datalek en ondervindt hiervan nog steeds hinder.

15. Mevrouw [redacted] heeft zich laten testen op 3 juli 2020 en op 9 september 2020. Zij heeft geen brief ontvangen van GGD GHOR, noch is zij op andere wijze geïnformeerd over het datalek. Mevrouw [redacted] is dus één van de gedupeerden van wie niet vaststaat dat persoonsgegevens zijn ontvreemd. Mevrouw [redacted] is slachtoffer geweest van een telefonische poging tot oplichting. Zij vermoedt dat de personen die haar belden haar gegevens hebben verkregen uit het GGD-datalek. Zij hadden de beschikking over informatie die mevrouw [redacted] met maar heel weinig personen en instanties deelt, maar die zij wel moest afgeven voor het maken van haar testafspraken.

16. Mevrouw [redacted] heeft zich op 18 februari 2021 laten testen en op 5 juli 2021 laten vaccineren. Ook zij heeft geen brief ontvangen van GGD GHOR en is ook niet op andere wijze door GGD GHOR geïnformeerd over het datalek. Mevrouw [redacted] is dus ook één van de gedupeerden van wie niet vaststaat dat persoonsgegevens zijn ontvreemd.

17. De heer [redacted] heeft zich in 2020 laten testen en op 16 juni 2021 en op 15 juli 2021 laten vaccineren. Sinds hij daarvoor afspraken maakte, heeft hij meerdere telefonische pogingen tot oplichting moeten doorstaan. Inmiddels is het zover dat hij geen telefoontjes meer durft aan te nemen van onbekende nummers. De heer [redacted] heeft geen brief ontvangen van GGD GHOR, noch is hij op andere wijze geïnformeerd over het datalek. Ook hij is dus één van de gedupeerden van wie niet vaststaat dat persoonsgegevens zijn ontvreemd.

3 DE AANGESCHREVEN PARTIJEN

18. Stichting ICAM c.s. schrijft naast de Staat ook de 25 GGD'en, de vereniging Publieke Gezondheid en Veiligheid Nederland en de stichting Projectenbureau Publieke Gezondheid en Veiligheid Nederland (gezamenlijk "**GGD GHOR**"), de 25 Veiligheidsregio's ("**Veiligheidsregio's**") en van ieder van de 25 GGD-regio's de grootste Gemeente ("**Gemeentes**") aan. Een volledig overzicht van de aangeschreven partijen kunt u vinden in **Bijlage 3**. De grondslagen worden hieronder uiteengezet in hoofdstuk 5. Of al deze partijen daadwerkelijk in een eventuele procedure zullen worden betrokken is mede afhankelijk van nader onderzoek en van de reactie op deze brief.

4 HET GGD-DATALEK

19. Op 16 september 2020 berichtte Nieuwsuur dat medewerkers van de GGD inzage hadden in alle persoonsgegevens die ten behoeve van testen en traceren waren opgeslagen.[8] Op 3 november 2020 berichtte het AD dat medewerkers van de GGD zichzelf ongeoorloofd toegang hadden verschaft tot de persoonlijke gegevens van bekende personen die geregistreerd stonden in het IT-systeem van de GGD.[9] Op 25 januari 2021 berichtte RTL Nieuws dat de persoonsgegevens in de GGD softwaresystemen toegankelijk waren voor onbevoegden, online te koop werden aangeboden en waarschijnlijk zijn verkocht aan internetcriminelen.

4.1 Getroffen systemen en persoonsgegevens

20. Het datalek betreft in ieder geval twee IT-systemen.

21. Ten eerste CoronIT, waarin testafspraken worden gemaakt en uitslagen worden teruggekoppeld aan mensen die getest zijn. CoronIT bevat onder meer naam, adres, woonplaats, telefoonnummer, e-mailadres, BSN, geslacht, geboortedatum, test- en/of vaccineerafspraken en testresultaten, contra-indicaties en COVID-19 klachten.[10]

22. Ten tweede HPZone (Lite), waarbinnen medewerkers ten behoeve van het uitvoeren van bron- en contactonderzoek in ieder geval toegang krijgen tot de gegevens van de GGD-regio waarvoor zij aan het werk zijn. In HP Zone (Lite) staan onder meer naam, adres, woonplaats, telefoonnummer, geslacht, geboortedatum en BSN. Verder wordt in HP Zone (Lite) ook informatie uit het

---

8 https://nos.nl/nieuwsuur/artikel/2348581-testlijnmedewerkers-kunnen-bij-persoonsgegevens-ook-als-dat-niet-mag en *Kamerstukken II* 2020-2021, 27 529, nr. 235, p. 1.

9 https://www.ad.nl/binnenland/ggd-medewerkers-gluurden-ongeoorloofd-naar-bners-in-coronadatabase~a12f2ae6/ en *Kamerstukken II* 2020-2021, 27 529, nr. 235, p. 1.

10 GGD GHOR FAQ, https://ggdghor.nl/thema/vragen-antwoorden-datadiefstal/, geraadpleegd op 24 december 2021.

bron- en contactonderzoek vastgelegd. Dit betreft onder andere 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.[11]

4.2 Omvang

23. Volgens GGD GHOR waren ten tijde van de berichtgeving van RTL Nieuws de persoonsgegevens van 5,5 miljoen mensen opgenomen in CoronIT, en de persoonsgegevens van 1 miljoen mensen in HPZone (Lite). Meer dan 26.000 (deels externe) callcentermedewerkers hadden toegang tot CoronIT en meer dan 20.000 tot HPZone (Lite).

24. RTL Nieuws heeft bekend gemaakt dat mensen die voor de GGD'en werkten, datasets met persoonsgegevens uit HPZone (Lite) en persoonsgegevens van individuele personen uit CoronIT online te koop hebben aangeboden.[12] De gegevens werden tegen betaling aangeboden via chatdiensten, zoals Telegram, Snapchat en Wickr, waarbij het mogelijk was om op verzoek de gegevens van een specifieke persoon of de gegevens van een geselecteerde groep van personen te ontvangen. Ook werden volgens RTL Nieuws complete datasets met (bijzondere) persoonsgegevens van tienduizenden mensen online aangeboden voor aanzienlijke bedragen. Deze datasets zijn zeer waardevol voor criminelen en zij vragen en/of bieden hier veel geld voor, omdat het uniek is dat op zo'n grote schaal BSN's worden verkocht.[13]

25. Volgens GGD GHOR zijn privégegevens van in ieder geval 1.250 mensen uit de coronasystemen gestolen en waarschijnlijk doorverkocht.[14] Volgens RTL Nieuws is het daadwerkelijke aantal gedupeerden echter veel groter[15] en wordt "*grootschalig gehandeld in de miljoenen adresgegevens, telefoonnummers en BSN's uit de twee coronasystemen van de GGD*".[16]

26. GGD GHOR heeft in 2020 aan KPMG opdracht gegeven een risicoanalyse op de systemen uit te voeren, waarvan de resultaten op 17 december 2020 zijn opgeleverd. De resultaten zijn niet publiekelijk beschikbaar en het is dus niet bekend welke risico's door KPMG zijn geconstateerd en of, en zo ja hoe, de Staat c.s. daarop heeft gehandeld. In ieder geval staat vast dat de beveiligingsmaatregelen niet op orde waren en nog steeds niet op orde zijn, zoals door de AP is geconcludeerd. Het GGD-datalek had eenvoudig voorkomen kunnen worden, althans de omvang had

---

11 GGD GHOR FAQ, https://ggdghor.nl/thema/vragen-antwoorden-datadiefstal/, geraadpleegd op 24 december 2021.
12 *Kamerstukken II* 2020-2021, 27 529, nr. 235, p. 1.
13 https://www.rtlnieuws.nl/nieuws/nederland/artikel/5210644/handel-gegevens-nederlanders-ggd-systemen-database-coronit-hpzone.
14 GGD GHOR FAQ, https://ggdghor.nl/thema/vragen-antwoorden-datadiefstal/, geraadpleegd op 24 december 2021.
15 https://www.rtlnieuws.nl/nieuws/nederland/artikel/5247728/datalek-datadiefstal-ggd-gedupeerden.
16 https://www.rtlnieuws.nl/nieuws/nederland/artikel/5210644/handel-gegevens-nederlanders-ggd-systemen-database-coronit-hpzone.

aanzienlijk beperkter kunnen zijn, indien de Staat c.s. elementaire IT-beveiligingsmaatregelen had getroffen, waarvan is vastgesteld dat deze geen impact zouden hebben gehad op de beschikbaarheid van de systemen, en indien zij adequate controles had uitgevoerd, hetgeen niet is gebeurd.

4.3 Kwetsbaarheden

4.3.1 Toegang en autorisaties

27. Onderdeel van de beveiliging van persoonsgegevens en het waarborgen van een passend beschermingsniveau vormt het voorkomen van ongeoorloofde toegang en het implementeren van een authenticatieproces. Ook autorisaties en het juiste beheer daarvan, zoals het tijdige aanpassen of intrekken van autorisaties, dragen bij aan een passend beveiligingsniveau. Het doel hiervan is dat medewerkers enkel toegang hebben tot persoonsgegevens die noodzakelijk zijn voor de uitvoering van hun taken.

28. Dat de toekenning van rechten in de GGD systemen te ruim was, is door de Staat erkend.[17] Alle circa 20.000 (deels externe) GGD-medewerkers hadden toegang tot gevoelige persoonsgegevens in HPZone (Lite).[18] In CoronIT konden circa 26.000 (deels externe) medewerkers meerdere dossiers inzien.[19] GGD-medewerkers hebben ook bevestigd dat zij toegang hadden tot gegevens (van andere GGD-regio's) waar zij geen toegang tot zouden moeten hebben.[20] Ook de AP heeft vastgesteld dat medewerkers over autorisaties beschikten die zij voor hun werkzaamheden niet of niet langer nodig hadden.[21]

29. Verder staat vast dat de exportfunctionaliteit in HPZone (Lite), waarmee grote hoeveelheden persoonsgegevens in bulk konden worden gedownload, toegankelijk was voor alle reguliere rollen.[22]

30. Ook bestond op het aanmaken van accounts die toegang hadden tot de systemen nauwelijks toezicht. Zo verklaarde een werknemer al "tientallen keren" een account te hebben laten aanmaken zonder enige controle en zonder dat een VOG ingeleverd was.[23]

---

17 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 93.
18 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 199.
19 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 13.
20 https://www.rtlnieuws.nl/tech/artikel/5211164/ggd-corona-systemen-toegang-vog-coronit-hpzone-light.
21 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ggd-moet-persoonsgegevens-beter-beschermen.
22 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 44.
23 https://www.rtlnieuws.nl/tech/artikel/5211164/ggd-corona-systemen-toegang-vog-coronit-hpzone-light. https://www.ad.nl/binnenland/ggd-medewerkers-gluurden-ongeoorloofd-naar-bners-in-coronadatabase~a12f2ae6/.

31. De toekenning van autorisaties en het juiste beheer daarvan zijn tot op heden niet op orde, zo bevestigt de AP. Zo heeft de AP naar aanleiding van het datalek geen duidelijk gedocumenteerde afspraken aangetroffen tussen de betrokken partijen ten aanzien van het toewijzen, wijzigen en intrekken van autorisaties. Bovendien heeft de AP geen toereikende documentatie aangetroffen die ten aanzien van HPZone (Lite) inzichtelijk maakt welke specifieke rechten en functionaliteiten aan de verschillende rollen in de autorisatiematrix zijn gekoppeld.[24]

32. De AP heeft voorts geconstateerd dat het mogelijk is CoronIT en HPZone (Lite) vanaf eigen apparatuur rechtstreeks te benaderen via een URL, derhalve zonder dat eerst behoeft te worden ingelogd op een beveiligde werkomgeving. Uit het onderzoek van de AP is in dat kader ook gebleken dat de onderzochte GGD'en laptops verstrekten aan een deel van hun medewerkers, terwijl er ook een grote groep medewerkers, waaronder medewerkers van de landelijke partners, op eigen apparatuur werkte. De AP heeft bevestigd hiervoor geen eenduidig beleid te hebben aangetroffen en GGD GHOR heeft aangegeven hierover met de landelijke partners geen afspraken te hebben vastgelegd.[25]

4.3.2 Export-, print- en zoekfunctionaliteiten

33. De GGD softwaresystemen beschikken over export-, print- en/of zoekfunctionaliteiten. Met de export- en printfuncties kunnen bestanden met persoonsgegevens in zijn geheel worden gedownload of geprint.[26] Daarbij bestaat ook de mogelijkheid om een bepaalde selectie van gegevens te maken.[27] De zoekfunctie biedt, althans bood, ruime mogelijkheden om op basis van minimale, algemeen bekende gegevens eenvoudig gericht naar personen te zoeken.

34. CoronIT beschikt alleen over een printfunctionaliteit. Deze printfunctionaliteit is volgens GGD GHOR met name aanwezig in het kader van noodprocedures, mocht zich een systeem- of internetstoring voordoen.[28] Volgens GGD GHOR is deze functionaliteit echter voor verschillende doeleinden gebruikt, onder andere door portiers en verkeersregelaars om te controleren of mensen een afspraak hebben.[29]

35. HPZone (Lite) beschikt zowel over een export- als een printfunctionaliteit.[30] De exportfunctionaliteit in HPZone (Lite) is kennelijk nodig om datasets te creëren voor statistische analyse en voor

---

24 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ggd-moet-persoonsgegevens-beter-beschermen.
25 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ggd-moet-persoonsgegevens-beter-beschermen.
26 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 44.
27 GGD GHOR FAQ, https://ggdghor.nl/thema/vragen-antwoorden-datadiefstal/, geraadpleegd op 24 december 2021.
28 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 17.
29 GGD GHOR FAQ, https://ggdghor.nl/thema/vragen-antwoorden-datadiefstal/, geraadpleegd op 24 december 2021.
30 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 243.

het genereren van databestanden voor opslag in een beveiligd datawarehouse. Deze functionaliteit is echter ook gebruikt voor het verdelen van werk over medewerkers. De printfunctionaliteit stelt medewerkers in staat om de informatie die op dat moment zichtbaar is op het scherm op te slaan als PDF. De printfunctionaliteit is voornamelijk gebruikt voor het overdragen van dossiers aan een andere GGD. Ook kan de functie worden gebruikt om een werklijst te printen.[31]

36. Alle GGD-medewerkers hadden toegang tot zowel de print- als de export- en zoekfunctionaliteiten, hetgeen voor de uitvoering van de werkzaamheden echter niet noodzakelijk was. Dat blijkt onder andere uit het feit dat het uitzetten van de print- en zoekfunctionaliteit in CoronIT geen problemen opleverde voor het operationeel proces.[32] De exportfunctionaliteit in HPZone (Lite) werd op 25 januari 2021 uitgezet en daarna voor een beperkt aantal medewerkers weer beschikbaar gemaakt, waarmee bevestigd is dat het niet nodig was dat alle GGD-medewerkers toegang hadden tot deze functionaliteit. De printfunctionaliteit in HPZone Lite is in eerste instantie niet uitgeschakeld, omdat dat grote gevolgen zou hebben voor de werkzaamheden. Deze functie is echter op 30 januari 2021 alsnog uitgezet.[33] Daaruit blijkt dat het ook ten aanzien van deze functionaliteit niet noodzakelijk was dat (alle) GGD-medewerkers er gebruik van konden maken.

37. Het feit dat deze functionaliteiten voor alle GGD-medewerkers algemeen toegankelijk waren en dat bovendien ongelimiteerde mogelijkheden bestonden om gegevens op te zoeken, te downloaden en te printen, maakten dat CoronIT en HPZone Lite zeer kwetsbaar waren/zijn voor datalekken. Dat risico heeft zich dan ook verwezenlijkt. Met gebruik van deze functies hebben GGD-medewerkers (bijzondere) persoonsgegevens van betrokkenen opgezocht, gedownload, online te koop aangeboden en waarschijnlijk verkocht.

4.3.3 Logging en monitoring

38. Het vastleggen van gebeurtenissen in logbestanden en regelmatige controle daarvan vormt een belangrijk onderdeel van informatiebeveiliging.[34] Ten aanzien van CoronIT en HPZone (Lite) is gebleken dat een deugdelijke en effectieve logging en controle ontbreekt.

39. Volgens de Staat c.s. is bij de bouw van HPZone en CoronIT bewust de keuze gemaakt om wel te loggen, maar om niet automatisch en continu te monitoren.[35] Minister de Jonge heeft verklaard dat GGD GHOR automatische fraudecontrole wel heeft overwogen, maar dit door tijdsdruk niet

---

31 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 17.
32 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 17 en *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 118.
33 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 118.
34 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ggd-moet-persoonsgegevens-beter-beschermen.
35 *Kamerstukken II* 2020-2021, 27 529/32 761, nr. 234, p. 20, vraag 102.

heeft kunnen implementeren. De implementatie stond uiteindelijk gepland voor maart 2021, nadat een eerdere poging was mislukt.[36]

40. Tot op heden worden er volgens het rapport van de AP echter nog steeds uitsluitend niet-automatische controles uitgevoerd. De AP heeft geconcludeerd dat er op de systemen van de GGD'en wel logbestanden werden gemaakt van de gebeurtenissen die in die systemen plaatsvinden, maar dat die logbestanden voorafgaand aan het GGD-datalek niet regelmatig zijn gecontroleerd. Daarbij heeft de AP überhaupt niet kunnen vaststellen of en door wie de logbestanden van HPZone Lite zijn gecontroleerd. De AP heeft daarnaast geconstateerd dat de logbestanden in CoronIT alleen in geval van een incident of klacht zijn gecontroleerd. Volgens medewerkers van de GGD'en ging het om niet-automatische, willekeurige checks waarbij zij bijvoorbeeld tijdens een videocall werd gevraagd om de digitale prullenbak te laten zien, om zo te controleren of daar vertrouwelijke gegevens in stonden.

41. In plaats van automatische controles heeft volgens de Staat c.s. inderdaad slechts steekproefsgewijze controle van de logging plaatsgevonden. In dat verband is aangegeven dat toegang en zoekopdrachten werden gelogd.[37] Indien uit de logging bleek dat ongeoorloofde handelingen waren uitgevoerd, werd dit aan de leidinggevende van de betrokken medewerker gemeld.[38] In het verleden heeft dat onder andere geleid tot het laten onderzoeken van de complete logging van CoronIT, het ontslaan van circa 30 medewerkers en het besluit om automatische en continue controle van de logging in te gaan richten.[39]

42. Hoewel de AP er dus van uit lijkt te gaan dat er wel logbestanden zijn aangemaakt, is het opmerkelijk dat noch de Staat, noch GGD GHOR tot op heden in staat is geweest om sluitend vast te stellen van hoeveel mensen gegevens onbevoegd zijn ingezien en/of gestolen. Kennelijk is de logging – als die inderdaad heeft plaatsgevonden – op zijn minst zeer gebrekkig geweest.

4.3.4 Gebrekkige overige beveiligingsmaatregelen

43. Uw voorganger heeft aangegeven dat de GGD'en verschillende beveiligingsmaatregelen zouden hebben geïmplementeerd. Zo zouden medewerkers trainingen hebben moeten volgen over privacy en gegevensbescherming, een Verklaring Omtrent Gedrag (VOG) moeten verstrekken en een geheimhoudingsovereenkomst moeten tekenen.[40] Uit verschillende bronnen blijkt echter dat deze beveiligingsmaatregelen in werkelijkheid niet (volledig en juist) zijn geïmplementeerd.

---

36 Zie onder andere de Eindbrief van de Autoriteit Persoonsgegevens aan GGD GHOR Nederland d.d. 8 november 2021, p. 6.
37 *Kamerstukken II* 2020-2021, 27 529/32 761, nr. 234, p. 26, vraag 130.
38 *Kamerstukken II* 2020-2021, 27 529/32 761, nr. 234, p. 10, vraag 42.
39 *Kamerstukken II* 2020-2021, 27 529/32 761, nr. 234, p. 48, vraag 226.
40 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vragen 7 en 241.

Zo sluit de GGD niet uit dat medewerkers toegang hebben gehad tot de systemen, nog voordat zij een VOG hadden overlegd,[41] dit terwijl de VOG werd gebruikt als screeningsmiddel.[42] Ook staat niet vast dat alle GGD-medewerkers een training omtrent privacy en gegevensbescherming hebben gehad,[43] of dat dat de screening van GGD-medewerkers in alle gevallen was afgerond voordat zij toegang hadden tot de systemen. Ook dit gebrek aan beveiligingsmaatregelen maakte de IT-systemen CoronIT en HPZone Lite kwetsbaar. Tezamen met het feit dat de toegangsrechten veel te ruim waren is daarmee een onaanvaardbaar risico genomen op misbruik van gegevens. Dat bij het uitbreiden van de personele capaciteit van de GGD GHOR en de verschillende GGD'en snelheid geboden was,[44] maakt het nog niet geoorloofd om de privacy en de gegevensbescherming van betrokkenen te veronachtzamen.

5 VERWERKINGSVERANTWOORDELIJKE(N)

44. In deze pararaaf zet Stichting ICAM c.s. eerst uiteen op welke gronden zij meent dat de Staat c.s. als de aansprakelijke partij dient te worden aangemerkt. Primair dient dit te worden getoetst aan de vraag welke partij(en) aangemerkt dienen te worden als verwerkingsverantwoordelijke(n) onder de AVG.

45. In artikel 4, aanhef en onder 7 AVG wordt het begrip verwerkingsverantwoordelijke gedefinieerd als volgt:

> *"een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen"*

46. Van gezamenlijke verantwoordelijkheid is sprake wanneer verschillende partijen voor specifieke verwerkingen gezamenlijk het doel, de wezenlijke onderdelen of de middelen vaststellen die een verwerkingsverantwoordelijke kenmerken.

5.1 Primair: de Staat

47. Stichting ICAM c.s. stelt zich primair op het standpunt dat de Staat (het ministerie van VWS) is aan te merken als zelfstandig verwerkingsverantwoordelijke in de zin van artikel 4 AVG.

---

41 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 8.
42 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 256.
43 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 257.
44 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 386.

48. Ten eerste heeft de Staat het doel van de gegevensverwerkingen door de GGD'en bepaald. Het testen op corona en het uitvoeren van bron- en contactonderzoek bij corona is geen wettelijke taak van de GGD'en. Ingevolge artikel 7 lid 1 van de Wet publieke gezondheid ("**Wpg**") ligt in geval van een epidemie van een infectieziekte behorend tot groep A, zoals het coronavirus, de leiding van de bestrijding van de epidemie bij de minister van VWS, die in dat verband (de voorzitters van) de Veiligheidsregio's kan instrueren hoe de bestrijding ter hand te nemen. De Staat heeft bij de uitbraak van de coronapandemie in Nederland echter de GGD'en gevraagd om in aanvulling op hun wettelijke taken inzake de infectieziektebestrijding, het testen en traceren van mensen met klachten die passen bij corona uit te voeren (ondanks dat zij niet voorbereid waren op een taak van deze omvang).[45]

49. Ten tweede heeft de Staat wezenlijke aspecten van de middelen voor gegevensverwerking vastgesteld. De Staat heeft in april/mei 2020 aan GGD GHOR de opdracht gegeven om CoronIT te ontwikkelen.[46] In dat kader heeft de Staat GGD GHOR specifieke aanwijzingen en instructies gegeven met betrekking tot de (door)ontwikkeling en inrichting van CoronIT, waaronder met betrekking tot het aansluiten van alle GGD'en, het geautomatiseerd bevestigen van afspraken, het delen van testuitslagen met betrokkenen, het doorsturen van gegevens naar de systemen Infectieziektebestrijding van de GGD'en (o.a. HPZone (Lite)) in het geval van een positieve test en het ontwikkelen van een koppelplatform gericht op gegevensuitwisseling met andere betrokken stakeholders.[47] Voorts heeft de Staat GGD GHOR opdracht gegeven een klantcontactcentrum op te richten om testafspraken te kunnen inplannen ter bestrijding van de coronapandemie.[48] Ten slotte blijkt uit de gang van zaken rondom de ontwikkeling van een vervanging voor HPZone Lite, dat de Staat ook bij de keuze voor dat systeem betrokken is geweest.[49]

---

45 *Kamerstukken II* 2020-2021, 27 529, nr. 235.

46 Feitenrelaas inzake gebeurtenissen omtrent coronatest-IT-systeem van de GGD, Dienstverleningsovereenkomst ARVODI-2018 - Opdracht aan GGD-GHOR voor het ontwikkelen en implementeren van CoronIT (bijlage bij de brief van de Minister van VWS aan de Tweede Kamer van 2 februari 2021, *Kamerstukken II*, 2020-2021, 27 529, 236).

47 Dienstverleningsovereenkomst ARVODI-2018 - Opdracht aan GGD-GHOR voor het ontwikkelen en implementeren van CoronIT, bijlage bij de brief van de Minister van VWS aan de Tweede Kamer van 2 februari 2021, *Kamerstukken II*, 2020-2021, 27 529, 236.

48 Dienstverleningsovereenkomst ARVODI-2018 opdracht aan GGD GHOR voor het doen oprichten van een klant contact centrum.

49 O.a. de Stand van zakenbrief digitale ondersteuning pandemiebestrijding, 12 februari 2021, GGD GHOR FAQ https://ggdghor.nl/thema/vragen-antwoorden-datadiefstal/, geraadpleegd op 24 december 2021 en https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_beveiliging_ggd_corona.pdf.

5.2 Subsidiair: gezamenlijke verantwoordelijkheid Staat met GGD GHOR, de GGD'en, de Veiligheidsregio's en/of de Gemeentes

50. Subsidiair stelt Stichting ICAM c.s. zich op het standpunt dat de Staat, de GGD GHOR, de GGD'en, de Veiligheidsregio's en/of de Gemeentes als (gezamenlijk) verwerkingsverantwoordelijken moeten worden aangemerkt.

5.2.1 GGD GHOR

51. Ten eerste is GGD GHOR aan te merken als (gezamenlijk) verwerkingsverantwoordelijke, onder andere omdat zij CoronIT heeft ontwikkeld en verantwoordelijk is voor het verstrekken van gebruiksrechten aan de GGD'en.[50] Ook heeft GGD GHOR HPZone Lite zodanig ingericht dat de GGD'en elkaar konden ondersteunen bij het bron- en contactonderzoek.[51] GGD GHOR presenteert zich bovendien als verwerkingsverantwoordelijke in haar communicatie, onder andere doordat zij een eigen privacyverklaring heeft en betrokkenen uit haar naam heeft geïnformeerd over het GDD-datalek.

5.2.2 De GGD'en

52. Ten tweede kwalificeren de 25 GGD'en als (gezamenlijk) verwerkingsverantwoordelijken, zoals ook wordt erkend door het ministerie van VWS, de GGD GHOR en de GGD'en zelf. De GGD'en zijn ingesteld door de colleges van burgermeester en wethouders ter uitvoering van specifieke taken voortvloeiend uit de Wpg, waaronder het verzamelen en verwerken van persoonsgegevens in het kader van infectieziektebestrijding. Naast de Wpg biedt ook de Wgbo een grondslag voor de kwalificatie van de GGD'en als (gezamenlijk) verwerkingsverantwoordelijken. De GGD'en treden immers op als zorgverlener waar het gaat om testen en vaccineren. Uit dien hoofde bestaat een behandelovereenkomst tussen de GGD en de betrokkene in de zin van de Wgbo. Die behandelovereenkomst vormt de basis voor de verwerking van persoonsgegevens. De GGD'en hanteren tot slot ieder een eigen privacyverklaring waarin zij zichzelf als verwerkingsverantwoordelijke kwalificeren en GGD GHOR heeft privacyverklaringen gepubliceerd waarin zij de GGD'en aanwijst als verwerkingsverantwoordelijken.[52]

---

50 *Kamerstukken II* 2020-2021, 27529; 32761, nr. 234, vraag 158.

51 GGD GHOR FAQ, https://ggdghor.nl/thema/vragen-antwoorden-datadiefstal/, geraadpleegd op 24 december 2021.

52 GGD GHOR, "Privacyverklaring testen op het coronavirus", te raadplegen via: https://ggdghor.nl/privacyverklaring-testenopcoronavirus/ en GGD GHOR, "Privacyverklaring landelijke capaciteit bron- en contactonderzoek COVID-19", te raadplegen via: https://ggdghor.nl/wp-content/uploads/2020/05/Privacy_Verklaring_BCO_April2021_Final.pdf.

5.2.3 De Veiligheidsregio's

53. Ten derde kunnen de Veiligheidsregio's aangemerkt worden als (gezamenlijk) verwerkingsverantwoordelijken. Ingevolge artikel 6 lid 2 Wpg draagt het bestuur van de veiligheidsregio zorg voor de voorbereiding op de bestrijding van een epidemie van een infectieziekte behorend tot groep A, zoals het coronavirus, en ingevolge lid 4 is het de voorzitter van de veiligheidsregio die zorg moet dragen voor de bestrijding zelf. Op grond van artikel 27 lid 1 Wpg moet de GGD de ontvangst van een melding als bedoeld in artikel 22 lid 1 Wpg onverwijld doorgeven aan de voorzitter van de veiligheidsregio. De GGD verstrekt daarbij op grond van artikel 27 lid 7 Wpg de gegevens, bedoeld in artikel 24 lid 1, 2 en 3, die deze nodig heeft voor de uitoefening van de hem bij de wet toegekende bevoegdheden.

5.2.4 De Gemeentes

54. Ten vierde kunnen de Gemeentes worden aangemerkt als (gezamenlijk) verwerkingsverantwoordelijken. Op grond van artikel 6 lid 1 Wpg draagt het college van burgemeester en wethouders zorg voor de uitvoering van de algemene infectieziektebestrijding. Tot die verplichting behoort in ieder geval het nemen van algemene preventieve maatregelen en het uitvoeren van bron- en contactopsporing bij meldingen als bedoeld in de artikelen 21, 22, 25 en 26 Wpg. Krachtens artikel 14 lid 1 Wpg dragen de colleges van burgemeester en wethouders van gemeentes die behoren tot een regio als bedoeld in de Wet veiligheidsregio's, zorg voor de instelling en instandhouding van een regionale gezondheidsdienst in die regio ter uitvoering van bij of krachtens de Wpg opgedragen taken (de GGD'en). De Gemeentes dienen toezicht te houden op de GGD'en en zijn eindverantwoordelijk voor de GGD'en.

6 SCHENDINGEN VAN HET RECHT DOOR DE STAAT c.s.

55. Gezien het bovenstaande meent Stichting ICAM c.s. dat er door de Staat c.s. ernstig, verwijtbaar en grootschalig inbreuk is gemaakt op een aantal wettelijke regelingen.

6.1 Geen passende beveiligingsmaatregelen (artikel 5 lid 1 sub f AVG en artikel 32 AVG)

56. Ten eerste heeft de Staat c.s. in strijd gehandeld met artikel 5 en artikel 32 van de Algemene verordening gegevensbescherming ("**AVG**").

57. Artikel 5 lid 1 onderdeel f AVG bevat het beginsel van vertrouwelijkheid en integriteit van persoonsgegevens. Artikel 32 lid 1 AVG werkt dit beginsel uit en verplicht de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen te treffen om een op het risico voor betrokkenen afgestemd beveiligingsniveau te waarborgen. Ingevolge het tweede lid wordt bij de beoordeling van het passende beveiligingsniveau met name rekening gehouden met

de verwerkingsrisico's. De Staat c.s. verwerkt in de GGD IT-systemen een grote hoeveelheid persoonsgegevens van miljoenen betrokkenen, waaronder BSN's en bijzondere persoonsgegevens zoals gezondheidsgegevens, waarvoor strengere beveiligings- en toestemmingsvereisten gelden. Gezien deze grootschalige verwerking van gevoelige en bijzondere persoonsgegevens was de beveiliging door de Staat c.s. ten tijde van de inbreuk niet passend, zoals bedoeld in artikel 32 AVG. De Staat c.s. heeft met name onvoldoende maatregelen genomen op het gebied van toegangsbeveiliging, autorisaties en autorisatiebeheer, logging en monitoring. Hierdoor heeft de Staat c.s. het ongeoorloofd doorzoeken, exporteren en printen van persoonsgegevens uit de systemen niet weten te voorkomen. De maatregelen die de Staat c.s. had kunnen en moeten nemen waren gezien de stand van de techniek en de uitvoeringskosten voorhanden. Het gebrek aan deze maatregelen heeft geleid tot een groot en ernstig (gerealiseerd) risico voor de rechten en vrijheden van betrokkenen.

6.2 Schending beginsel dataminimalisatie (artikel 5 lid 1 sub c AVG)

58. Ten tweede heeft de Staat c.s. het beginsel van dataminimalisatie, neergelegd in artikel 5 lid 1 sub c AVG, in ernstige mate geschonden.

59. De Staat dient zich conform artikel 5 lid 1 sub c AVG te beperken tot de verwerking van uitsluitend die persoonsgegevens die toereikend, ter zake dienend en noodzakelijk zijn voor het doel waarvoor zij worden verwerkt. De Staat c.s. had op basis van een beoordeling van de noodzaak moeten beperken wie er toegang hadden tot persoonsgegevens en welke soorten toegang er werd verleend. Ook had zij ervoor moeten zorgen dat functionaliteiten alleen toegankelijk waren voor degenen voor wie dit noodzakelijk was. Daartoe had zij een werkend proces voor beveiliging, screening van medewerkers en het aanpassen en intrekken van autorisaties moeten implementeren en uitvoeren. Dat is niet gebeurd, zelfs niet nadat haar dat door de AP werd opgedragen.

6.3 Schending verantwoordingsplicht (artikel 5 lid 2 AVG en artikel 24 AVG)

60. Ten derde heeft de Staat c.s. in strijd gehandeld met hun verantwoordingsplicht.

61. Een verwerkingsverantwoordelijke moet op grond van artikel 5 lid 2 AVG kunnen aantonen dat hij de beginselen neergelegd in artikel 5 lid 1 AVG naleeft. In dat kader dient de verwerkingsverantwoordelijke ingevolge artikel 24 lid 1 AVG passende maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Artikel 24 lid 2 AVG werkt dat uit door te bepalen dat een verwerkingsverantwoordelijke dient te beschikken over een passend gegevensbeschermingsbeleid, dat ook uitgevoerd wordt. Het voorgaande betekent dat de Staat c.s., gezien de grootschalige verwerking van (bijzondere) persoons-

gegevens, dient te beschikken over een concreet en eenduidig (beveiligings)beleid, een schriftelijke procedure en duidelijke afspraken met de landelijke partners met betrekking tot toegangsbeveiliging, (het aanpassen en intrekken van) autorisaties en autorisatiebeheer, logging en monitoring en het gebruik van eigen apparatuur. Hieraan ontbreekt het tot op de dag van vandaag.

6.4 Gegevensbescherming door ontwerp en door standaardinstellingen (artikel 25 AVG)

62. Ten vierde heeft de Staat c.s. in strijd gehandeld met de beginselen van *privacy by design* en *privacy by default*, zoals neergelegd in artikel 25 AVG.

63. Bij het ontwerp van CoronIT in 2020 zou *security by design* en *privacy by design* zijn meegenomen. CoronIT beschikt echter over een printfunctionaliteit en was toegankelijk voor 26.000 medewerkers. Na het bekend worden van het GGD-datalek heeft men de printfunctie uitgeschakeld, zodat de GGD'en alleen nog lijsten kunnen maken vanuit een beveiligde omgeving. De Staat c.s. heeft bevestigd dat het uitzetten van de printfunctionaliteit geen problemen opleverde voor het operationeel proces.

64. Bij het ontwerp van HPZone zou *privacy by design* niet zijn meegenomen, aangezien het systeem dateert uit 2003. HPzone Lite is echter pas in augustus 2020 geïmplementeerd. HPZone Lite heeft zowel een export- als een printfunctionaliteit. Na het GGD-datalek is ook de print- en exportfunctie van HPZone Lite uitgeschakeld en daarna alleen beschikbaar gesteld aan een beperkte groep medewerkers die deze functionaliteit daadwerkelijk nodig heeft voor de uitvoering van de werkzaamheden. Ook de te ruime toegangsrechten en het gebrek aan adequate logging en monitoring zijn aan te merken als gebrekkig implementatie van de beginselen van *privacy* en *security by design* en *by default*.

65. Zowel ten aanzien van CoronIT als HPZone (Lite) zijn pas na het GGD-datalek maatregelen genomen die al bij ingebruikname van de systemen in het kader van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen hadden kunnen en moeten worden getroffen. Deze maatregelen hadden bovendien eenvoudig doorgevoerd kunnen worden, met geen tot minimale impact op het operationele proces. Dat HPZone uit 2003 dateert doet aan deze verplichting niets af.

6.5 Schending beroepsgeheim GGD (artikel 7:457 BW)

66. Ten vijfde heeft de Staat c.s. in strijd gehandeld met de Wet inzake de geneeskundige behandelingsovereenkomst ("**Wgbo**").

67. De Wgbo is van toepassing wanneer sprake is van een behandelingsovereenkomst (artikel 7:446 lid 1 BW). Artikel 7:457 lid 1 BW bepaalt dat de hulpverlener ervoor zorg dient te dragen dat aan anderen dan de patiënt geen inlichtingen over de patiënt of inzage in of afschrift van de gegevens

uit het dossier worden verstrekt, behoudens toestemming van de patiënt. Uitgangspunt is dat iedereen die in de gezondheidszorg werkzaam is een geheimhoudingsplicht heeft. De geheimhoudingsplicht geldt niet alleen voor de individuele arts, maar ook voor de zorginstelling, die er op zijn beurt voor moet zorgen dat zijn medewerkers deze verplichting nakomen.[53] Bij het testen en vaccineren treedt de GDD op als hulpverlener.[54] De GGD heeft in dat kader een behandelingsovereenkomst met de betrokkene[55] en dient geheimhouding te betrachten ten aanzien van het medisch dossier. Desondanks hadden GGD-medewerkers toegang tot gegevens (van andere GGD-regio's) waar zij geen toegang tot zouden moeten hebben.[56]

6.6 Schending beveiligingseisen Wabvpz

68. Ten zesde heeft de Staat c.s. in strijd gehandeld met de beveiligingseisen die voortvloeien uit de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg ("**Wabvpz**").

69. Op grond van artikel 8 lid 1 Wabvpz neemt de zorgaanbieder het BSN van de patiënt in zijn administratie op bij het vastleggen van persoonsgegevens met betrekking tot de verlening van zorg. Artikel 10 Wabvpz jo. artikel 2 Regeling gebruik Burgerservicenummer in de zorg bepaalt dat de verwerking van het BSN door zorgverleners moet voldoen aan de NEN 7510. Ingevolge artikel 15j Wabvpz jo. artikel 3 lid 2 van het Besluit elektronische gegevensverwerking in de zorg ("**Begz**") draagt een zorgaanbieder, overeenkomstig de NEN 7510 en NEN 7512, zorg voor een veilig en zorgvuldig gebruik van zorginformatiesystemen. Overeenkomstig artikel 5 lid 1 Begz draagt de zorgaanbieder er tevens zorg voor dat de logging voldoet aan het bepaalde in NEN 7513.

70. Door de AP is duidelijk uitgedragen dat de NEN 7510 een belangrijke norm voor informatiebeveiliging in de zorg is.[57] Relevante beheersmaatregelen volgens de NEN 7510 zijn onder andere de volgende:

i) Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's;
ii) De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden;

---

53 R.P. Wijne, GS Bijzondere overeenkomsten, art. 7:457 BW, aant. 3.
54 *Kamerstukken II* 2020-2021, 27 529/32 761, nr. 234, p. 8, vraag 32. Zie ook: Rechtbank Noord-Holland 12 april 2017, ECLI:NL:RBNHO:2017:2838.
55 *Kamerstukken II* 2020-2021, 27 529/32 761, nr. 234, p. 8, vraag 34.
56 https://www.rtlnieuws.nl/tech/artikel/5211164/ggd-corona-systemen-toegang-vog-coronit-hpzone-light.
57 Autoriteit Persoonsgegevens, Besluit tot het opleggen van een bestuurlijke boete aan OLVG, 26 november 2020.

iii) Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie;
iv) Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging;
v) Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen;
vi) Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn;
vii) Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken;
viii) Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken;
ix) Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen;
x) De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast;
xi) Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging;
xii) Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure;
xiii) Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

71. NEN 7510 schrijft niet exact voor op welke wijze gelogd moet worden, maar de NEN 7513 vult de NEN 7510 op dat punt nader in.

72. Zoals in het voorgaande reeds uiteen is gezet, zijn er bij de GGD'en onvoldoende beheersmaatregelen geïmplementeerd op het gebied van toegangsbeveiliging, autorisaties en autorisatiebeheer, screening en training van medewerkers, logging van de gebruikte systemen en controle op deze logging. De Staat c.s. voldoet ten aanzien van de verwerking van persoonsgegevens in HPZone Lite en CoronIT derhalve niet aan de NEN 7510 en NEN 7513.

7 AANSPRAKELIJKHEID EN SCHADE

7.1 Aansprakelijkheid op grond van de AVG

73. Stichting ICAM c.s. stelt op grond van artikel 80 en 82 AVG (i) primair de Staat zelfstandig, en (ii) subsidiair de Staat c.s. hoofdelijk aansprakelijk voor alle schade die de gedupeerden hebben geleden door de privacyinbreuken ten gevolge van het GGD-datalek. De grondslagen daarvoor zijn de volgende.

74. Iedere betrokkene die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op de AVG, heeft het recht om op grond van artikel 82 AVG van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade. Artikel 80 AVG, in samenhang met nationaal recht, biedt Stichting ICAM, als organisatie zonder winstoogmerk die actief is op het gebied van de bescherming van de rechten en vrijheden van de betrokkene in verband met de bescherming van diens persoonsgegevens, het recht om deze schadevergoeding namens de gedupeerden te vorderen.

75. Uit artikel 82 lid 2 AVG volgt dat elke verwerkingsverantwoordelijke die bij de verwerking betrokken is, aansprakelijk is voor de schade die wordt veroorzaakt door een schending van de AVG. Wanneer meerdere verwerkingsverantwoordelijken bij dezelfde verwerking betrokken zijn, wordt elke verwerkingsverantwoordelijke krachtens artikel 82 lid 3 AVG voor de gehele schade aansprakelijk gehouden, teneinde te garanderen dat de schade van de betrokkene daadwerkelijk wordt vergoed.

76. Op grond van de AVG dient de verwerkingsverantwoordelijke *alle* schade te vergoeden die iemand kan lijden ten gevolge van een verwerking die inbreuk maakt op de AVG. Daarbij dient, in het licht van de rechtspraak van het Hof van Justitie, het begrip "schade" ruim te worden uitgelegd, op een wijze die ten volle recht doet aan de doelstellingen van de AVG.[58] Uit overweging 85 AVG volgt dat een inbreuk in verband met persoonsgegevens kan resulteren in lichamelijke, materiële of immateriële schade voor natuurlijke personen, zoals verlies van controle over hun persoonsgegevens of de beperking van hun rechten, discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongeoorloofde ongedaanmaking van pseudonimisering, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie. Ten gevolge van het GGD-datalek heeft zich zowel materiële als immateriële schade voorgedaan.

77. Daarnaast en in aanvulling op artikel 82 AVG doet Stichting ICAM c.s. een beroep op artikel 6:96 en 6:106 BW.

---

[58] Overweging 146 AVG.

78. Artikel 6:96 lid 1 BW bepaalt dat materiële schade zowel geleden verlies als gederfde winst omvat. De gedupeerden van het GGD-datalek hebben recht op vergoeding van geleden materiële schade als gevolg van het GGD-datalek. Deze schade heeft betrekking op kosten die betrokkenen hebben gemaakt om de schade die als gevolg van het GGD-datalek kan worden verwacht te voorkomen of te beperken en om de aard en omvang van de schade vast te stellen, waaronder tijd die aan het onderzoeken en afhandelen van (de gevolgen van) het GGD-datalek is besteed, aan contact met de GGD en Stichting ICAM met vragen over het datalek, aan het bestuderen van de door GGD GHOR ter beschikking gestelde informatie en aan het controleren van de gegevens van (verdachte) telefoontjes/e-mails na het datalek. Het GGD-datalek leidt bovendien tot materiële schade met betrekking tot betrokkenen die slachtoffer zijn geworden van identiteitsdiefstal of phishing als gevolg van het GGD-datalek.

79. Ingevolge artikel 6:106 lid 1 BW heeft de benadeelde recht op een naar billijkheid vast te stellen schadevergoeding indien hij lichamelijk letsel heeft opgelopen, in zijn eer of goede naam is geschaad of op andere wijze in zijn persoon is aangetast.

80. Van de in artikel 6:106 lid 1 aanhef en onder b BW bedoelde aantasting "op andere wijze" kan sprake zijn indien de aard en de ernst van de normschending en van de gevolgen daarvan voor de benadeelde dat met zich meebrengen. Deze persoonsaantasting hoeft niet met concrete gegevens te worden onderbouwd, indien de aard en de ernst van de normschending meebrengen dat de in dit verband relevante nadelige gevolgen daarvan voor de benadeelde zo voor de hand liggen dat een aantasting in de persoon kan worden aangenomen.[59] Daarvan is in dit geval sprake. Subsidiair biedt Stichting ICAM c.s. bewijs aan van deze geleden schade.

81. Het GGD-datalek betreft een zeer grootschalige inbreuk op de AVG, waarbij gevoelige gegevens zoals het BSN en bijzondere persoonsgegevens zoals gezondheidsgegevens van miljoenen burgers toegankelijk zijn geweest voor datadiefstal. Bovendien duurt deze inbreuk nu al bijna twee jaar voort, terwijl de verantwoordelijken al vanaf het begin op de hoogte zijn van de slechte beveiliging. Na de berichtgeving over het GGD datalek door *RTL Nieuws* bleek dat vanaf het begin van de coronapandemie al bekend was dat de GGD softwaresystemen niet adequaat waren beveiligd, maar daaraan lange tijd niets is gedaan. Op 29 januari 2021 citeerde RTL Nieuws GGD GHOR-voorzitter André Rouvoet:

> *"Dat het registratiesysteem van de GGD niet veilig is, was bekend. Vóór corona was dat geen probleem. Maar nu maken er duizenden mensen gebruik van, en daar is het systeem niet geschikt voor. [...] Het is verschrikkelijk dat dit heeft kunnen gebeuren, dat spijt ons. [...] We zijn enorm geschrokken dat medewerkers zich hebben laten verleiden om gegevens naar buiten te brengen. De systemen gaven daar ruimte voor, dat trekken wij ons aan. [...] Tijdens de tweede golf hebben we besloten om door te gaan met dit systeem, om snel te*

[59] Hoge Raad 19 maart 2019, ECLI:NL:HR:2019:376, *NJ* 2019/162 (*X/EBI*).

kunnen blijven werken. Dat was een verkeerde keuze, want het was niet veilig genoeg te maken."[60]

82. Er is bovendien door GGD-medewerkers verklaard dat zij sinds de zomer van 2020 al kritiek hebben geuit over de vrije toegang tot de systemen en grote hoeveelheid aan gegevens, maar dat die kritiek stelselmatig werd genegeerd.[61] Deze onzorgvuldigheid in de omgang met bijzonder gevoelige gegevens zowel als de toegankelijkheid door ex-GGD medewerkers is nog steeds een groot probleem.[62]

7.2 Aansprakelijkheid op grond van artikel 6:162 BW

83. Voorts stelt Stichting ICAM c.s. de Staat, althans de Staat c.s., aansprakelijk op grond van artikel 6:162 BW. In overweging 146 AVG is bepaald dat de AVG eventuele eisen tot schadeloosstelling wegens inbreuken op andere regels in het EU-recht of het nationale recht onverlet laat. Het behoort aldus tot de mogelijkheden om een vordering op grond van artikel 6:162 BW in te stellen, parallel aan een vordering op grond van de AVG. Artikel 6:162 BW dient daarbij, voor zover nodig, conform de AVG te worden uitgelegd. In dit geval is voldaan aan alle vereisten die artikel 6:162 BW stelt.

84. Er is sprake van een onrechtmatige daad omdat de Staat c.s. heeft gehandeld in strijd met een wettelijke verplichting en bovendien in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt. Bij dit laatste is vooral van belang dat sprake is geweest van zeer laks handelen, waarbij de Staat c.s. gedurende een langere periode de meest basale beveiligingsmaatregelen niet heeft doorgevoerd en daarmee heeft geaccepteerd dat zeer gevoelige gegevens van miljoenen mensen onvoldoende beveiligd waren.

85. Aan het relativiteitsvereiste is evident voldaan. De normen uit de AVG strekken immers ter bescherming van de privacyrechtelijke belangen van de gedupeerden van het GGD-datalek.

86. Voorts kan de onrechtmatige gedraging aan de Staat c.s. worden toegerekend. Het uitgangspunt in de AVG is dat de mate van schuld er in beginsel niet toe doet, aangezien het een risicoaansprakelijkheid betreft: het enkele feit dat door een verwerking de AVG wordt geschonden, is voldoende om aansprakelijk te worden gehouden voor de schade die het gevolg is van die schending. Dit heeft tot gevolg dat aan het vereiste van toerekening is voldaan, nu artikel 6:162 BW (en artikel 6:163 BW) zoveel mogelijk conform de AVG dient te worden uitgelegd. Bovendien is

60 https://www.rtlnieuws.nl/nieuws/nederland/artikel/5211580/rouvoet-ggd-datalek-gegevens-gestolen-onderzoek-privacy.
61 https://www.rtlnieuws.nl/tech/artikel/5211164/ggd-corona-systemen-toegang-vog-coronit-hpzone-light.
62 https://www.gelderlander.nl/home/ggd-laks-met-beschermen-privacy-oud-medewerker-kan-vanuit-huis-bij-jouw-gegevens~a922a62b/ en https://www.vpngids.nl/nieuws/ggd-heeft-privacyzaakjes-nog-altijd-niet-op-orde/.

aan het vereiste van toerekening voldaan, nu de schendingen van de AVG aan de Staat c.s. kunnen worden toegerekend krachtens schuld. Het is immers aan hen te wijten dat de gedupeerden de controle over hun persoonsgegevens zijn verloren en in hun privacybelangen zijn geschaad.

87. Tot slot is ook aan het vereiste van een causaal verband voldaan. Aangezien artikel 6:162 BW (en artikel 6:98 BW) conform de AVG dient te worden uitgelegd, geldt dat het causaal verband aangenomen wordt. In het kader van de AVG is immers gekozen voor een risicoaansprakelijkheid. Subsidiair geldt dat een vermoeden van causaal verband dient te worden aangenomen tussen de onrechtmatige daad en de schade die de gedupeerden hebben geleden. Er is immers sprake van schending van een norm die ertoe strekt een specifiek gevaar ter zake van het ontstaan van schade bij een ander te voorkomen, en dit specifieke gevaar heeft zich heeft verwezenlijkt. De normen die zijn opgenomen in de AVG hebben als voornaamste doel de bescherming van persoonsgegevens te verhogen en rechten van betrokkenen te verstevigen. De AVG sterkt tot bescherming van persoonsgegevens onder meer om te voorkomen dat natuurlijke personen de controle over hun persoonsgegevens verliezen en schade lijden. Indien het causaal verband niet op voorhand wordt aangenomen, geldt meer subsidiair dat er evengoed een causaal verband bestaat tussen de schade en het onrechtmatig handelen. De schade die de gedupeerden hebben geleden, is immers veroorzaakt door de inbreukmakende handelingen van de Staat c.s. dan wel doordat de Staat c.s. heeft gehandeld in strijd met een maatschappelijke zorgvuldigheidsnorm.

8 AANSPRAKEN EN IN TE STELLEN VORDERINGEN

88. Op grond van het voorgaande meent Stichting ICAM c.s. dat de Staat c.s. gehouden is om **op de kortst mogelijke termijn** maatregelen te nemen en medewerking te verlenen aan het maken van afspraken met Stichting ICAM c.s., met een strekking zoals in nr. 89 opgesomd sub (d) t/m (i). De wijze waarop de Staat c.s. uitvoering dient te geven aan deze maatregelen en de termijn waarbinnen deze maatregelen volledig dienen te zijn uitgevoerd, kunnen in nader overleg met Stichting ICAM c.s. worden bepaald.

89. Indien de Staat c.s., in de visie van Stichting ICAM c.s., de genoemde maatregelen onvoldoende (tijdig) uitvoert, is Stichting ICAM c.s. voornemens om een (collectieve) vordering tegen de Staat c.s. in te stellen, voor wat betreft Stichting ICAM op grond van artikel 3:305a BW. Zij zal alsdan in ieder geval het volgende vorderen, waar mogelijk hoofdelijk en onder verbeurte van dwangsommen:

a) Een verklaring voor recht dat primair de Staat zelfstandig en subsidiair de Staat c.s. gezamenlijk, inbreuk heeft gemaakt en nog steeds maakt op de AVG, waaronder op artikel 5, artikel 24, artikel 25 en artikel 32 AVG;
b) Een verklaring voor recht dat primair de Staat en subsidiair de Staat c.s. onrechtmatig heeft gehandeld in de zin van artikel 6:162 BW;

c) Een verklaring voor recht dat primair de Staat zelfstandig en subsidiair de Staat c.s. jegens alle gedupeerden aansprakelijk is voor de schade veroorzaakt door het GGD-datalek;

d) Een bevel tot het beëindigen en beëindigd houden van alle inbreuken op de AVG en van al het onrechtmatig handelen in verband met de beveiliging van persoonsgegevens in de computersystemen die door de GGD'en worden gebruikt bij de bestrijding van de coronapandemie, onder andere door passende beveiligingsmaatregelen te implementeren en passend beleid vast te stellen en uit te voeren, afgestemd op de risico's voor de betrokkenen;

e) Een bevel dat primair de Staat en subsidiair de Staat c.s. door onafhankelijke en te goeder naam en faam bekend staande forensische IT-experts, te benoemen op voordracht van de Staat c.s. en goed te keuren door Stichting ICAM, nader onderzoek dient te laten doen naar de omvang van het GGD-datalek, waaronder omtrent de vraag van welke personen de persoonsgegevens onbevoegd zijn of kunnen worden ingezien, zijn ontvreemd, te koop zijn aangeboden en/of zijn verkocht;

f) Een bevel dat primair de Staat en subsidiair de Staat c.s. van alle in het kader van vorderingen sub d) en e) genomen maatregelen en onderzoeken schriftelijk en gedetailleerd verslag dient te doen aan Stichting ICAM en controle daarvan door een onafhankelijke en te goeder naam en faam bekend staande deskundige dient toe te staan, en daartoe alle medewerking dient te verlenen;

g) Een bevel dat primair de Staat en subsidiair de Staat c.s. alle betrokkenen van wie mogelijk persoonsgegevens onbevoegd zijn ingezien, ontvreemd, te koop zijn aangeboden en/of zijn verkocht, individueel dient te informeren over het GGD-datalek en de (mogelijke) gevolgen en risico's daarvan;

h) Een bevel dat primair de Staat en subsidiair de Staat c.s. primair aan alle gedupeerden van het GGD-datalek en subsidiair aan de bij Stichting ICAM aangesloten deelnemers, een schadevergoeding dient te betalen ter hoogte van € 500,- voor iedere persoon van wie persoonsgegevens toegankelijk en/of beschikbaar zijn geweest voor onbevoegden en/of mogelijk zijn ontvreemd, te koop zijn aangeboden en/of zijn verkocht, en een schadevergoeding ter hoogte van € 1.500,- voor iedere persoon van wie komt vast te staan dat persoonsgegevens onbevoegd zijn ingezien, ontvreemd, te koop zijn aangeboden en/of zijn verkocht, een en ander te vermeerderen met wettelijke rente;

i) Een bevel dat primair de Staat en subsidiair de Staat c.s. aan Stichting ICAM de volledige kosten dient te vergoeden die zij heeft moeten maken en nog zal moeten maken om voor zichzelf en/of voor alle gedupeerden naleving van bovenbedoelde rechten (te trachten) af te dwingen, om ervoor te zorgen dat de rechten van de gedupeerden worden geëerbiedigd en om ervoor te zorgen dat de gedupeerden een passende vergoeding voor de door hen geleden schade ontvangen, waaronder de kosten voor (externe) financiering van de betreffende kosten, de hoogte van welke kosten door Stichting ICAM op een later moment nader onderbouwd zal worden.

90. Op basis van de thans bekende informatie is sprake is van ten minste ongeveer 6,5 miljoen gedupeerden waarvan persoonsgegevens toegankelijk waren voor onbevoegden en mogelijk zijn ontvreemd, te koop zijn aangeboden en/of zijn verkocht en van ten minste ongeveer 1.250 gedupeerden waarvan vaststaat dat persoonsgegevens zijn ontvreemd, te koop zijn aangeboden en (mogelijk) zijn verkocht. Op basis daarvan bedraagt de schadevordering voor alle gedupeerden gezamenlijk, zoals vermeld in sommatie h), tenminste € 3.251.875.000,- (te vermeerderen met wettelijke rente en vergoeding van de kosten). Voor de gedupeerden die zich als deelnemer bij Stichting ICAM hebben aangemeld bedraagt de schadevordering per heden ten minste € 30.000.000,- (te vermeerderen met wettelijke rente en vergoeding van de kosten), waarbij ervan uit wordt gegaan dat zich daaronder geen personen bevinden van wie vaststaat dat persoonsgegevens zijn ontvreemd, hetgeen echter wel het geval is.

9 SOMMATIES

9.1 Beschikbaar houden van gegevens

91. Teneinde alle gedupeerden van het GGD-datalek een compensatie voor de door hen geleden schade te kunnen betalen, is het van groot belang dat de gegevens van die personen beschikbaar zijn en blijven ten behoeve van dat doel.

92. Namens Stichting ICAM c.s. verzoeken, en zo nodig sommeren wij de Staat c.s. dan ook om **binnen acht weken na dagtekening van deze brief** schriftelijk aan ondergetekenden te bevestigen dat de Staat c.s. de hierna genoemde gegevens van alle personen van wie persoonsgegevens in de relevante GGD-systemen toegankelijk en/of beschikbaar waren voor onbevoegden en (mogelijk) zijn ontvreemd, te koop zijn aangeboden en/of zijn verkocht, te bewaren en beschikbaar te houden voor zolang dat nodig is om tot volledige en correcte uitbetaling van schadevergoedingen over te kunnen gaan. De Staat c.s. dient daartoe **binnen diezelfde termijn** een kopie van die gegevens te (laten) maken en veilig te (laten) stellen in het bijzijn van een deurwaarder en een onafhankelijke en te goeder naam en faam bekend staande IT-deskundige, te benoemen op voordracht van de Staat c.s. en goed te keuren door Stichting ICAM. De deurwaarder zal daarvan proces-verbaal opmaken en de IT-deskundige zal daarvan een rapport opmaken, welk proces-verbaal en welk rapport aan Stichting ICAM zal worden verstrekt. Een en ander dient per persoon de volgende gegevens te betreffen:

a) Voor- en achternaam;
b) Geboortedatum;
c) Adres;
d) E-mailadres en telefoonnummer, indien beschikbaar;
e) De gegevens die toegankelijk en/of beschikbaar waren voor onbevoegden en (mogelijk) zijn ontvreemd, te koop zijn aangeboden en/of zijn verkocht;

f) De periode waarin de betreffende gegevens toegankelijk waren voor onbevoegden;

g) Het aantal personen dat (onbevoegd) toegang had tot de betreffende gegevens en de motivering daarvan, mede in het licht van hun rollen of functies;

h) Informatie over de vraag of de betreffende gegevens daadwerkelijk of waarschijnlijk zijn ontvreemd, te koop zijn aangeboden en/of zijn verkocht of anderszins zijn aangewend op een wijze die tot aansprakelijkheid van de Staat c.s. jegens gedupeerden leidt.

9.2 Informatieverstrekking

9.2.1 Betrokkenheid en rol van de verschillende partijen

93. In hoofdstuk 5 is uiteengezet dat en waarom Stichting ICAM c.s. zich primair op het standpunt stelt dat de Staat aansprakelijk is voor de schade van de gedupeerden van het GGD-datalek, alsmede waarom Stichting ICAM c.s. zich subsidiair op het standpunt stelt dat de Staat c.s. hoofdelijk aansprakelijk is. Dat standpunt is gebaseerd op publiek beschikbare informatie. Teneinde te kunnen beoordelen of die informatie, relevant voor de beoordeling welke partijen in welke mate kunnen worden aangemerkt als verwerkingsverantwoordelijken op grond van de AVG, juist en volledig is, is het voor Stichting ICAM c.s. van belang daarover nadere informatie te ontvangen. U bent op grond van artikel 21 en artikel 843a Rv verplicht deze informatie aan haar te verstrekken.

94. Namens Stichting ICAM c.s. verzoeken, en zo nodig sommeren wij de Staat c.s. dan ook om haar **binnen acht weken na dagtekening van deze brief** aan ondergetekenden alle informatie en documenten te verstrekken die noodzakelijk of nuttig kunnen zijn bij het vaststellen van de (feitelijke en formele) betrokkenheid, rol en verantwoordelijkheden van iedere (rechts)persoon en instantie die betrokken is geweest bij de verwerking van persoonsgegevens in de relevante GGD-systemen.

9.2.2 Informatie over de beveiliging van de systemen en de genomen maatregelen

95. Stichting ICAM c.s. stelt zich op het standpunt dat de Staat c.s. op basis van de hierboven uiteengezette feiten, inbreuk heeft gemaakt op verschillende wettelijke bepalingen en rechtsregels. Haar stellingname is voor een groot deel gebaseerd op publiek beschikbare informatie. Teneinde nader zicht te krijgen op de door de Staat c.s., zowel voorafgaand aan als na publiekelijk bekend worden van het GGD-datalek, genomen organisatorische en technische beveiligingsmaatregelen, wenst Stichting ICAM c.s. daarover nadere informatie te ontvangen. U bent op grond van artikel 21 en artikel 843a Rv verplicht deze informatie aan haar te verstrekken.

96. Namens Stichting ICAM c.s. verzoeken, en zo nodig sommeren wij de Staat c.s. dan ook om **binnen acht weken na dagtekening van deze brief** aan ondergetekenden alle informatie en documenten te verstrekken die noodzakelijk of nuttig kunnen zijn bij het vaststellen van de door de Staat c.s., zowel voorafgaand aan als na publiekelijk bekend worden van het GGD-datalek, genomen organisatorische en technische beveiligingsmaatregelen ten aanzien van de persoonsgegevens in de (IT-)systemen die door de GGD'en zijn of worden gebruikt in het kader van testen, vaccineren en bron- en contactonderzoek, waaronder in ieder geval begrepen:

a) Alle offerteaanvragen, programma's van eisen, offertes en overeenkomsten, inclusief bijlagen, met betrekking tot de (door)ontwikkeling, implementatie en uitrol van CoronIT, HPZone en/of HPZone Lite;
b) Alle offerteaanvragen, programma's van eisen, offertes en overeenkomsten, inclusief bijlagen, met betrekking tot de inrichting en instandhouding van een klantcontactcentrum voor test- en vaccinatieafspraken en bron- en contactonderzoek;
c) Alle offerteaanvragen, programma's van eisen, offertes en overeenkomsten, inclusief bijlagen, met betrekking tot de uitbesteding aan derde partijen van klantcontact- en/of callcenterwerkzaamheden;
d) Informatie over de verschillen in beveiliging tussen het reeds voor de coronacrisis bestaande systeem HPZone en het later ontwikkelde HPZone Lite;
e) Data Protection Impact Assessments (DPIA) ten aanzien van CoronIT, HPZone en HPZone Lite;
f) Door de Staat c.s. gehanteerde beveiligings- of privacybeleid omtrent het omgaan met CoronIT en HPZone (Lite), met persoonsgegevens en met datalekken in verband met testen, vaccineren en bron- en contactonderzoek, waaronder het beleid ten aanzien van toegangsrechten en autorisatiebeheer en logging en monitoring;
g) Informatie en documenten met betrekking tot de training van (externe) medewerkers ten aanzien van het gebruik van CoronIT en HPZone (Lite) en de omgang met persoonsgegevens, waaronder beleid, protocollen, instructies en presentaties;
h) Audits, rapportages en onderzoeken (intern of door derde partijen) met betrekking tot privacy(risico's) en beveiliging(srisico's) in verband met CoronIT, HPZone en HPZone Lite;
i) Informatie over eerdere signaleringen (onder meer van GGD-medewerkers) dat de informatiebeveiliging in het kader van het testen, vaccineren en bron- en contactonderzoek niet op orde was, en over het gevolg dat daaraan is gegeven;
j) Audits, rapportages en onderzoeken (intern of door derde partijen) ten aanzien van de effectiviteit van (beveiligings)maatregelen doorgevoerd na publiek bekend worden van het datalek;
k) Informatie en documenten over het onderzoek dat heeft plaatsgevonden naar de omvang van de groep gedupeerden en de potentiële schadelijke gevolgen van het datalek.

10 UITNODIGING TOT OVERLEG

97. Namens Stichting ICAM c.s. hebben wij in deze brief uiteengezet wat de aanspraken van Stichting ICAM c.s. zijn en wat de motivering daarvoor is.

98. Stichting ICAM c.s. acht het in het belang van alle betrokkenen partijen indien deze kwestie in goed overleg, buitengerechtelijk, kan worden opgelost. Om die reden nodigt Stichting ICAM c.s. de Staat c.s. hierbij dan ook – voor wat Stichting ICAM betreft mede op de voet van artikel 3:305a lid 3 sub c BW - uit om met haar in overleg te treden over de hierboven omschreven kwestie. Wij verzoeken u om ons **binnen drie weken na dagtekening van deze brief** te informeren of u bereid bent tot dergelijk overleg.

99. Bij gebreke van een tijdige bevestiging van uw bereidheid tot overleg of indien het bedoelde overleg niet **binnen een termijn van acht weken na dagtekening van deze brief** kan plaatsvinden en tot een voor Stichting ICAM c.s. acceptabele uitkomst of bevredigende vervolgafspraken leidt, acht Stichting ICAM c.s. zich vrij om de rechtsmaatregelen te treffen die zij nodig acht.

100. Deze brief is bedoeld om een beroep te doen op de rechten van alle gedupeerden van het GGD-datalek, om die rechten te behouden en om die rechten zo nodig af te dwingen. Deze brief dient derhalve mede te worden beschouwd als een stuiting van enige lopende verjaringstermijn in de zin van artikel 3:317 BW.

101. Stichting ICAM c.s. behoudt zich in dit stadium alle rechten en weren voor, voor wat betreft Stichting ICAM zowel voor zichzelf als namens en ten behoeve van alle gedupeerden van het GGD-datalek.

102. Wij verzoeken u alle correspondentie over deze zaak te zenden aan Douwe Linders (linders@solv.nl), Yentl van den Winkel (winkel@solv.nl) en Lora Mourcous (mourcous@solv.nl).

Hoogachtend,

[redacted]

SOLV Advocaten
mr. D.M. Linders
mr. Y. van den Winkel
mr. L. Mourcous