DAGVAARDING

Heden, de achtentwintigste maart tweeduizenddrieëntwintig;

heb ik,

Ten verzoeke van:

De **STICHTING INITIATIEVEN COLLECTIEVE ACTIES MASSASCHADE (ICAM)**, statutair gevestigd te Amsterdam en kantoorhoudende aan het adres Maliesingel 17, 3581 BD te Utrecht te dezer zake domicilie kiezende aan het adres Anne Frankstraat 121, 1018 BZ te Amsterdam ten kantore van SOLV Advocaten, van wie mr. D.M. Linders, mr. Y. van den Winkel en mr. A.L.M. Bakhuis in deze zaak als advocaten namens eiseres zullen optreden en als zodanig worden gesteld, hierna te noemen "**Stichting ICAM**",

GEDAGVAARD:

1) De **STAAT DER NEDERLANDEN**, in het bijzonder het Ministerie van Volksgezondheid, Welzijn en Sport, zetelende te 's-Gravenhage, die woonplaats heeft gekozen ten kantore van mr. [redacted] en mr. [redacted], advocaten verbonden aan Pels Rijcken, kantoorhoudende aan het adres Bezuidenhoutseweg 57, 2594 AC te 's-Gravenhage, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

2) De vereniging met volledige rechtsbevoegdheid **PUBLIEKE GEZONDHEID EN VEILIGHEID NEDERLAND**, statutair gevestigd te Utrecht en kantoorhoudende aan het adres Zwarte Woud 2, 3524 SJ te Utrecht, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

3) De stichting **STICHTING PROJECTENBUREAU PUBLIEKE GEZONDHEID EN VEILIGHEID NEDERLAND**, statutair gevestigd te Utrecht en kantoorhoudende aan het adres Zwarte Woud 2, 3524 SJ te Utrecht, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

4) De stichting **STICHTING VERENIGINGSBUREAU PUBLIEKE GEZONDHEID EN VEILIGHEID NEDERLAND**, statutair gevestigd te Utrecht en kantoorhoudende aan het adres Zwarte Woud 2, 3524 SJ te Utrecht, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

5) De stichting **STICHTING LANDELIJKE COÖRDINATIE COVID-19 BESTRIJDING**, statutair gevestigd te gemeente Utrecht en kantoorhoudende aan het adres Zwarte Woud 2, 3524 SJ te Utrecht, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

6) De **GEMEENTELIJKE GEZONDHEIDSDIENST (GGD) AMSTERDAM-AMSTELLAND**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Amsterdam, en kantoorhoudende aan het adres Nieuwe Achtergracht 100, 1018 WT te Amsterdam, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

7) De **GGD BRABANT-ZUIDOOST**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Eindhoven, en kantoorhoudende aan het adres Clausplein 10, 5611 XP te Eindhoven, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

8) De **DIENST GEZONDHEID & JEUGD ZUID-HOLLAND ZUID**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Dordrecht, en kantoorhoudende aan het adres Karel Lotsyweg 40, 3318 AL te Dordrecht, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

9) De **GGD DRENTHE**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Assen, en kantoorhoudende aan het adres Mien Ruysweg 1, 9408 KA te Assen, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

10) De **GGD FLEVOLAND**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Lelystad, en kantoorhoudende aan het adres Noorderwagenstraat 2, 8223 AM te Lelystad, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

11) De **VEILIGHEIDSREGIO FRYSLÂN**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Leeuwarden, en kantoorhoudende aan het adres Harlingertrekweg 58, 8913 HR te Leeuwarden, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

12) De **VEILIGHEIDS- EN GEZONDHEIDSREGIO GELDERLAND-MIDDEN (VGGM)**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Arnhem, en kantoorhoudende aan het adres Eusebiusbuitensingel 43, 6828 HZ te Arnhem, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

13) De **GGD GELDERLAND-ZUID**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Nijmegen, en kantoorhoudende aan het adres Groenewoudseweg 275, 6524 TV te Nijmegen, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

14) De **GGD GOOI & VECHTSTREEK**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Bussum, en kantoorhoudende aan het adres Burgemeester de Bordesstraat 80, 1404 GZ te Bussum, gemeente Gooise Meren, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

15) De **GGD GRONINGEN**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Groningen, en kantoorhoudende aan het adres Hanzeplein 120, 9713 GW te Groningen, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

16) De **GEMEENSCHAPPELIJKE REGELING GEMEENTELIJKE GEZONDHEIDSDIENST EN VEILIG THUIS HAAGLANDEN**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te 's-Gravenhage, en kantoorhoudende aan het adres Westeinde 128, 2512 HE te 's-Gravenhage, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

17) De **GGD HART VOOR BRABANT**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te 's-Hertogenbosch, en kantoorhoudende aan het adres Pettelaarpark 10, 5216 PD te 's-Hertogenbosch, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

18) De **REGIONALE DIENST OPENBARE GEZONDHEIDSZORG HOLLANDS MIDDEN**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Leiden, en kantoorhoudende aan het adres Parmentierweg 49, 2316 ZV te Leiden, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

19) De **GEMEENTELIJKE GEZONDHEIDSDIENST HOLLANDS NOORDEN**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Alkmaar, en kantoorhoudende aan het adres Hertog Aalbrechtweg 22, 1823 DL te Alkmaar, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

20) De **GGD IJSSELLAND**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Zwolle, en kantoorhoudende aan het adres Zeven Alleetjes 1, 8011 CV te Zwolle, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

21) De **VEILIGHEIDSREGIO KENNEMERLAND**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Haarlem, en kantoorhoudende aan het adres Zijlweg 200, 2015 CK te Haarlem, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

22) De **VEILIGHEIDSREGIO LIMBURG-NOORD**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Venlo, en kantoorhoudende aan het adres Nijmeegseweg 42, 5916 PT te Venlo, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

23) De **GGD NOORD- EN OOST-GELDERLAND**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Warnsveld, en kantoorhoudende aan het adres Rijksstraatweg 65, 7231 AC te Warnsveld, gemeente Zutphen, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

24) De **GGD REGIO UTRECHT**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Zeist, en kantoorhoudende aan het adres De Dreef 5, 3706 BR te Zeist, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

25) De **GGD ROTTERDAM-RIJNMOND**, ingeschreven in het handelsregister onder vestigingsnummer 000022962077, kantoorhoudende aan het adres Schiedamsedijk 95, 3011 EN te Rotterdam, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

26) **SAMENTWENTE**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Enschede, en kantoorhoudende aan het adres Nijverheidstraat 30, 7511 JM te Enschede, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

27) De **GGD WEST-BRABANT**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Breda, en kantoorhoudende aan het adres Doornboslaan 225, 4816 CZ te Breda, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

28) De **GGD ZAANSTREEK-WATERLAND**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Zaandam, en kantoorhoudende aan het adres Vurehout 2, 1507 EC te Zaandam, gemeente Zaanstad, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

29) De **GEMEENSCHAPPELIJKE GEZONDHEIDSDIENST ZEELAND**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Goes, en kantoorhoudende aan het adres Westwal 37, 4461 CM te Goes, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

30) De **GENEESKUNDIGE GEZONDHEIDSDIENST ZUID-LIMBURG**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Heerlen, en kantoorhoudende aan het adres Het Overloon 2, 6411 TE te Heerlen, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

31) De **VEILIGHEIDSREGIO AMSTERDAM-AMSTELLAND**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Amsterdam, en kantoorhoudende aan het adres Ringdijk 98, 1097 AH te Amsterdam, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

32) De **VEILIGHEIDSREGIO ROTTERDAM-RIJNMOND**, een publiekrechtelijke rechtspersoon (openbaar lichaam op basis van gemeenschappelijke regeling), zetelend te Rotterdam, en kantoorhoudende aan het adres Wilhelminakade 947, 3072 AP te Rotterdam, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

33) De **GEMEENTE AMSTERDAM**, een publiekrechtelijke rechtspersoon, gemeente, zetelende te Amsterdam en kantoorhoudende aan het adres Amstel 1, 1011 PN te Amsterdam, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

34) De **GEMEENTE ROTTERDAM**, een publiekrechtelijke rechtspersoon, gemeente, zetelende te Rotterdam en kantoorhoudende aan het adres Coolsingel 40, 3011 AD te Rotterdam, aldaar mijn exploot doende en afschrift dezes, exclusief producties, latende aan:

OM:

Op woensdag 5 juli 2023 (de "roldatum"), des ochtends om 10.00 uur, niet in persoon maar vertegenwoordigd door een advocaat, te verschijnen ter openbare civiele terechtzitting van de rechtbank Amsterdam, team Civiel recht, afdeling handelszaken, alsdan te houden in één van de lokalen van het gerechtsgebouw aan het adres Parnassusweg 280, 1076 AV te Amsterdam,

MET AANZEGGING DAT:

a) indien een gedaagde verzuimt advocaat te stellen of het hierna te noemen griffierecht niet tijdig betaalt, en de voorgeschreven termijnen en formaliteiten in acht zijn genomen, de rechtbank tegen deze gedaagde verstek zal verlenen en de hierna omschreven vordering zal toewijzen, tenzij deze haar onrechtmatig of ongegrond voorkomt;

b) indien ten minste één van de gedaagden in het geding verschijnt en het griffierecht tijdig heeft voldaan, tussen alle partijen één vonnis wordt gewezen, dat als een vonnis op tegenspraak wordt beschouwd;

c) bij verschijning in het geding van ieder der gedaagden een griffierecht zal worden geheven, te voldoen binnen vier weken te rekenen vanaf het tijdstip van verschijning;

d) de hoogte van de griffierechten is vermeld in de meest recente bijlage behorend bij de Wet griffierechten burgerlijke zaken, die onder meer is te vinden op de website: www.kbvg.nl/griffierechtentabel;

e) van een persoon die onvermogend is, een bij of krachtens de wet vastgesteld griffierecht voor onvermogenden wordt geheven, indien hij op het tijdstip waarop het griffierecht wordt geheven heeft overgelegd:

   i) een afschrift van het besluit tot toevoeging, bedoeld in artikel 29 van de Wet op de rechtsbijstand, of indien dit niet mogelijk is ten gevolge van omstandigheden die redelijkerwijs niet aan hem zijn toe te rekenen, een afschrift van de aanvraag, bedoeld in artikel 24, tweede lid, van de Wet op de rechtsbijstand; dan wel

   ii) een verklaring van het bestuur van de raad voor rechtsbijstand, bedoeld in artikel 7, derde lid, onderdeel e, van de Wet op de rechtsbijstand waaruit blijkt dat zijn inkomen niet meer bedraagt dan de inkomens bedoeld in de algemene maatregel van bestuur krachtens artikel 35, tweede lid, van die wet;

f) van gedaagden die bij dezelfde advocaat verschijnen en gelijkluidende conclusies nemen of gelijkluidend verweer voeren, op basis van artikel 15 van de Wet griffierechten burgerlijke zaken slechts eenmaal een gezamenlijk griffierecht wordt geheven;

g) eiseres op straffe van niet-ontvankelijkheid verplicht is deze dagvaarding aan te tekenen in het centraal register voor collectieve acties als bedoeld in artikel 3:305a lid 7 BW;

h) deze aantekening tot gevolg heeft dat - tenzij de rechtbank eiseres aanstonds niet ontvankelijk verklaart - de rechtbank de zaak aanhoudt totdat een termijn van drie maanden na de aantekening in het centraal register is verstreken;

i) na het verstrijken van deze termijn de behandeling van de zaak wordt voortgezet in de stand waarin zij zich bevindt, tenzij ingevolge artikel 1018d lid 2 Rv deze termijn is verlengd of een andere collectieve vordering voor dezelfde gebeurtenis is ingesteld;

j) de in artikel 128 lid 2 Rv bedoelde roldatum voor het nemen van de conclusie van antwoord door de rechtbank zal worden bepaald op een termijn van zes weken nadat de in artikel 1018c lid 3 Rv bedoelde termijn is verstreken;

k) de producties behorende bij deze dagvaarding op de eerstdienende dag in het geding zullen worden gebracht,

TENEINDE:

Te antwoorden op de volgende vorderingen van eiseres:

INHOUDSOPGAVE

DEFINITIES EN AFKORTINGEN (TEVENS PRODUCTIE A.1)

AP	Autoriteit Persoonsgegevens.
AVG	Verordening (EU) 2016/679 (Algemene Verordening Gegevensbescherming).
BCO	Bron- en contactonderzoek in verband met corona.
Begz	Besluit elektronische gegevensverwerking door zorgaanbieders.
Betrokkenen	Betrokkenen zoals gedefinieerd in artikel 4 sub 1) AVG.
BSN	Burgerservicenummer.
Claimcode 2019	E. Bauw en J. van Mourik, *Claimcode 2019*, Den Haag: Boom Juridisch 2019.
CoronIT	Softwaresysteem voor het plannen van test- en vaccinatieafspraken in verband met corona.
Deelnemers	Bij Stichting ICAM door middel van de Deelnemersovereenkomst aangesloten Gedupeerden.
Deelnemersovereen-komst	De overeenkomst die een Deelnemer met Stichting ICAM sluit wanneer deze zich voor de collectieve actie over het GGD-datalek aanmeldt via de Website (producties B.11 en B.12).
DPG	Een directeur publieke gezondheid van een GGD zoals benoemd krachtens artikel 14 Wpg.
DPIA	Een gegevensbeschermingseffectbeoordeling zoals omschreven in artikel 35 AVG.
EDPB	De European Data Protection Board ingesteld krachtens artikel 68 AVG, bestaande uit de voorzitters van de toezichthoudende autoriteiten van iedere lidstaat en de Europese Toezichthouder voor gegevensbescherming.
EVRM	Europees Verdrag voor de Rechten van de Mens.
Exclusieve Belangenbehartiger	De exclusieve belangenbehartiger zoals bedoeld in artikel 1018e lid 1 Rv.

Financier	Liesker Procesfinanciering B.V. te Breda.
Financieringsovereen-komst	De overeenkomst procesfinanciering tussen Stichting ICAM en de Financier d.d. 12 juli 2021.
Gedupeerden	De Gedupeerden Categorie A en de Gedupeerden Categorie B.
Gedupeerden Categorie A	Alle natuurlijke personen van wie persoonsgegevens zijn verwerkt in één van of beide GGD-systemen in de periode tussen ingebruikname daarvan in verband met de bestrijding van corona en 1 februari 2021, bijvoorbeeld omdat zij een afspraak hebben gemaakt bij een GGD om te testen of vaccineren in verband met corona of omdat zij onderdeel zijn geweest van bron- en contactonderzoek in verband met corona, met uitzondering van de personen die deel uitmaken van Gedupeerden Categorie B.
Gedupeerden Categorie B	Alle natuurlijke personen van wie persoonsgegevens zijn verwerkt in één van of beide GGD-systemen in de periode tussen ingebruikname daarvan in verband met de bestrijding van corona en 1 februari 2021, bijvoorbeeld omdat zij een afspraak hebben gemaakt bij een GGD om te testen of vaccineren in verband met corona of omdat zij onderdeel zijn geweest van bron- en contactonderzoek in verband met corona, en waarvan vaststaat of zal worden vastgesteld dat hun persoonsgegevens als gevolg van het GGD-datalek door ongeautoriseerde personen zijn ingezien of bij ongeautoriseerde personen in handen zijn gekomen, zoals door het ongeoorloofd inzien, downloaden, exporteren, printen, kopiëren, fotograferen en/of, aanbieden, verhandelen, ontvangen of op andere wijze delen van de persoonsgegevens.
Gemeenten	Gedaagden 33 en 34.
GGD'en	Gedaagden 6 t/m 30.
GGD GHOR	Gedaagden 2 t/m 5.
GGD-systemen	CoronIT en HPZone Lite.
HPZone Lite	Softwaresysteem dat door de GGD'en werd en/of wordt gebruikt voor het uitvoeren van bron- en contactonderzoek in verband met corona.
minister	De minister van Volksgezondheid, Welzijn en Sport.

ministerie	Het ministerie van Volksgezondheid, Welzijn en Sport.
Raad van Bestuur	De Raad van Bestuur van Stichting ICAM.
Raad van Toezicht	De Raad van Toezicht van Stichting ICAM.
Staat c.s.	Gedaagden 1 t/m 34.
Statuten	De statuten van Stichting ICAM d.d. 25 november 2021 (productie B.1).
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming.
Veiligheidsregio's	Gedaagden 31 en 32.
Verantwoordings-document	Het verantwoordingsdocument van Stichting ICAM, waarin zij uiteenzet op welke wijze zij voldoet aan de vereisten van artikel 3:305a BW en invulling geeft aan de Claimcode 2019 (productie B.8).
VOG	Verklaring Omtrent het Gedrag.
Wabvpz	Wet aanvullende bepalingen in de zorg.
WAMCA	Wet afwikkeling massaschade in collectieve actie.
Website	De website van Stichting ICAM met informatie over deze collectieve actie, te vinden via www.datalek-ggd.nl (productie B.3).
Wgbo	Wet Geneeskundige Behandelingsovereenkomst.
Woo-stukken	De door de GGD'en openbaargemaakte stukken zoals door Stichting ICAM overgelegd in productiecategorie G.
Wpg	Wet publieke gezondheid.

1 INLEIDING

1.1 Kern van deze zaak

1. Stichting ICAM behartigt de belangen van ruim 6,5 miljoen mensen van wie zeer privacygevoelige informatie blootgesteld is geweest aan diefstal. Het betreft persoonsgegevens uit de IT-systemen van de GGD'en, verzameld en gebruikt in verband met de bestrijding van corona. Stichting ICAM wordt actief gesteund door 133.691 Deelnemers. Zij willen meer zorgvuldigheid van de Nederlandse overheid bij de omgang met gevoelige informatie van burgers, opheldering over de exacte omvang en impact van het GGD-datalek en compensatie voor de schade die het datalek heeft veroorzaakt voor alle getroffenen.

2. Deze WAMCA-zaak betreft het grootste en ernstigste datalek in de Nederlandse geschiedenis, veroorzaakt door laakbaar handelen en nalaten door de Nederlandse overheid.

3. In januari 2021 werd bekend dat de IT-systemen die de GGD'en gebruiken in verband met corona, ernstige beveiligingsgebreken bevatten. Persoonsgegevens van zeker 6,5 miljoen mensen waren gedurende ten minste elf maanden onnodig en vermijdbaar toegankelijk voor ongeveer 35.000 in allerijl ingeschakelde tijdelijke GGD-medewerkers, waaronder veel nieuwe en extern ingehuurde krachten. De betreffende medewerkers kregen na een gebrekkige screening toegang tot veel meer gegevens dan nodig was voor hun werkzaamheden, waaronder naam en adresgegevens, telefoonnummers, e-mailadressen, BSN-nummers en gegevens over besmettingen en vaccinatiestatus, achterliggende medische klachten, werksituatie en nauwe contactpersonen.[1]

4. De activiteiten van de GGD-medewerkers in de systemen werden niet afdoende gelogd en gemonitord. Zij konden daardoor ongemerkt omvangrijke databestanden met gevoelige persoonsgegevens van 6,5 miljoen Nederlanders inzien, kopiëren en downloaden.[2]

5. Dat dit datalek heeft plaatsgevonden, staat tussen partijen niet ter discussie.[3] Door de slechte beveiliging - in strijd met onder meer de AVG - zijn persoonsgegevens van een grote groep mensen op onrechtmatige wijze langdurig blootgesteld geweest aan diefstal. Hierdoor hebben de Gedupeerden de controle over hun persoonsgegevens verloren. Ze weten dat hun persoonsgegevens voor een zeer grote groep ongeautoriseerde personen toegankelijk zijn geweest; ze weten niet of ze daadwerkelijk gestolen zijn en verder misbruikt zijn of nog gaan worden. Internetcriminelen gebruiken persoonsgegevens voor identiteitsfraude, oplichting, *phishing* en intimidatie. Wanneer gegevens in handen komen van verkeerde partijen, brengt dat bovendien risico's met zich mee van stigmatisering, uitsluiting en discriminatie. Te denken valt

1 Paragrafen 3.1, 3.3, 4.2.4.2 en 4.2.4.3.
2 Paragrafen 3.1.10, 3.4 en 4.2.4.4.
3 Randnummer 36.

aan de situatie dat gegevens over onderliggende gezondheidsproblematiek – zoals een Hiv-besmetting – terechtkomen bij (potentiële) werkgevers, verzekeraars of buitenlandse regimes.

6. Ook staat niet ter discussie dat daadwerkelijk persoonsgegevens ontvreemd zijn en in het criminele circuit zijn beland: dat is het geval.[4] Daarvoor zouden ook vier personen zijn veroordeeld (**productie F.15**). Voor zover tot nu toe door Gedaagden is erkend en meegedeeld, zou dat (slechts) een groep van circa 1.250 personen betreffen. Er zijn echter sterke aanwijzingen dat deze informatie onvolledig is en dat die groep personen beduidend groter is. De belangrijkste aanwijzing zijn de bevindingen van RTL Nieuws. RTL Nieuws heeft contact gehad met internetcriminelen, waarbij haar bestanden met gegevens zijn aangeboden van veel meer dan 1.250 personen (**productie C.17**):

> "De datadiefstal bij de GGD treft veel meer mensen dan het aantal gedupeerden dat de organisatie publiekelijk meldt. […] het daadwerkelijk aantal gedupeerden is echter veel groter, en de GGD heeft na maanden nog geen goed beeld van hoe groot de datadiefstal nu echt is, blijkt uit onderzoek van RTL Nieuws. […] RTL Nieuws heeft willekeurig verschillende mensen opgebeld van wie hun gegevens door criminelen te koop zijn aangeboden. Deze gegevens zijn afkomstig uit twee coronasystemen van de GGD: CoronIT, dat wordt gebruikt voor testen en vaccinaties, en HPZone Lite, het systeem dat wordt gebruikt voor het bron- en contactonderzoek. De personen zijn allemaal niet door de GGD geïnformeerd over dat hun gegevens uit de systemen van de GGD zijn gestolen en mogelijk verhandeld. […] De databestanden, met in totaal de privégegevens van zo'n 600 personen, waren volgens de aanbieders een voorproefje van de vele duizenden tot tienduizenden personen die konden worden geleverd."

7. De impact van het datalek moet niet onderschat worden. Het betreft (i) veel Gedupeerden, (ii) bijzondere, gevoelige en veel persoonsgegevens, (iii) een schending van de wet door de overheid, die Gedupeerden bij uitstek zouden moeten kunnen vertrouwen en (iv) databases waarvan Gedupeerden de facto geen keuze hebben of ze erin willen staan of niet: het verstrekken van bijzondere persoonsgegevens aan de Gedaagden is onvermijdelijk, in ieder geval indien iemand getest of gevaccineerd wil worden.

8. Vanwege al deze factoren is het voor de Gedupeerden en voor de maatschappij in het algemeen van belang dat duidelijkheid wordt gegeven over wat er gebeurd is. Onder meer daartoe dient deze procedure. Stichting ICAM stelt met dit doel voor ogen een aantal incidentele vorderingen in (paragraaf 1.6 en hoofdstuk 10).

9. De oorzaak van het GGD-datalek is dat de Gedaagden jarenlang onvoldoende hebben gedaan om hun IT-systemen goed te beveiligen. Zij hebben verzuimd om in de GGD-systemen ook maar de meest basale beveiligingsmaatregelen te nemen.

10. Stichting ICAM waardeert vanzelfsprekend de enorme inspanning die de rijksoverheid en de GGD'en in de bestrijding van de coronapandemie hebben geleverd. Ook heeft zij begrip voor het

[4] Randnummer 36.

argument dat de corona-testcapaciteit op korte termijn moest worden uitgebreid en dat dit uitdagingen met zich meebracht, waaronder op het terrein van informatiebeveiliging. Dat alles neemt echter niet weg dat Gedaagden eerder, sneller en betere maatregelen hadden kunnen en behoren te nemen:

l) Paraat staan voor uitbraak van infectieziekten. De Staat c.s. hadden de GGD-systemen vooraf beter kunnen en behoren in te richten, zodat deze bestand waren geweest tegen een situatie zoals de coronapandemie. Het is immers niet zo dat een omvangrijke infectieziekte-uitbraak zoals de coronapandemie door de Staat c.s. niet had kunnen en zelfs was voorzien. De (betreffende afdelingen bij) de Gedaagden ontlenen hun bestaansrecht aan het bestrijden, niet alleen reactief, maar ook proactief, van dit type ziekten. Lang voordat de eerste coronabesmetting plaatsvond, wist men al dat de dag zou komen dat er een grote epidemie of pandemie zou uitbreken en dat de verouderde GGD-systemen dan niet geschikt en veilig zouden zijn. Het is de taak en verantwoordelijkheid van de Staat c.s. om daar binnen redelijke grenzen zo goed mogelijk op voorbereid te zijn. In een crisissituatie zoals de coronapandemie is het immers veel moeilijker om zaken in de hand te houden, terwijl het belang van goede informatiebeveiliging juist dan exponentieel toeneemt. Bovendien hadden alle landen ter wereld te maken met dezelfde crisis en voor zover Stichting ICAM bekend is het nergens zo fout gegaan als in Nederland;

m) Snellere oplossing van de beveiligingsgebreken. De Staat c.s. hadden het datalek sneller kunnen en behoren op te lossen. Het lek heeft onnodig lang bestaan, terwijl de Staat c.s. reeds lang op de hoogte waren van de risico's en de potentiële gevolgen van de slechte beveiliging. De Staat c.s. zijn er meerdere malen op gewezen dat de persoonsgegevens van miljoenen mensen gevaar liepen.[5] Ook toen namen zij nog geen toereikende maatregelen om de (wettelijk laakbare) gebreken te herstellen. In ieder geval had, toen de pandemie uitbrak, gelijktijdig óók de beveiliging van de bijzondere persoonsgegevens van de personen in de betreffende databases een belangrijk speerpunt moeten worden. De GGD-systemen zijn vanaf maart (HPZone) c.q. juni (CoronIT) 2020 ingezet. In de richtsnoeren die de European Data Protection Board uitvaardigde in april 2020 benadrukte de EDPB al het belang van gegevensbescherming bij het bestrijden van het coronavirus.[6] In februari 2021 schreef KPMG in een advies aan GGD-koepelorganisatie GGD GHOR, op basis van onderzoek dat slechts twee dagen in beslag heeft genomen (**productie G.56**):

> "Gebruik van HPZone dient zo snel mogelijk te worden stopgezet. Met het huidige systeem en de genomen beheersmaatregelen kan geen, bij de persoonsgegevens passend, adequaat beveiligingsniveau worden bereikt."

[5] Paragraaf 3.1.
[6] EDPB, 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak', aangenomen op 21 april 2020, p. 3.

11. Pas in januari 2021, nadat RTL Nieuws haar eerste conclusies publiceerde, werden de ernstigste beveiligingsgebreken verholpen. De minister zei daarover in het Kamerdebat over het GGD-datalek het volgende (**productie C.13**):

> "Het is niet zo dat er niks is gebeurd, maar we hebben er onvoldoende aandacht voor gehad. […] Ik had daar zelf scherper bovenop moeten zitten. Dit lag - met alle veelheid van taken - niet bovenop de stapel, dat had wel gemoeten. Had het eerder gekund, had het eerder gemoeten? Ja."

12. De Staat c.s. hebben onvoldoende gedaan en te laat ingegrepen. Zelfs nu nog schieten de Staat c.s. substantieel te kort in de beveiliging van persoonsgegevens van Nederlandse ingezetenen.

13. Er is naar de overtuiging van Stichting ICAM sprake geweest van bijzonder verwijtbaar handelen (hoewel dat voor het vaststellen van aansprakelijkheid in deze zaak geen vereiste is). Na het bekend worden van het datalek zijn wel maatregelen genomen om de beveiliging te verbeteren, maar van het werkelijk nemen van verantwoordelijkheid en van een zichtbare beleidsmatige en praktische wijziging in de aanpak en preventie van dit soort problemen is – ondanks de enorme impact op Betrokkenen - nog niets gebleken.

1.2 Belang en doel van deze zaak

14. Stichting ICAM is een artikel 3:305a-belangenorganisatie. Zij komt in deze procedure op voor de belangen van alle natuurlijke personen van wie persoonsgegevens zijn verwerkt in één of beide GGD-systemen ten tijde van het GGD-datalek (de Gedupeerden, zoals gedefinieerd in **productie A.1**). Deze groep personen valt uiteen in twee categorieën:

a) Personen waarvan onzeker is of hun persoonsgegevens als gevolg van het GGD-datalek zijn ontvreemd (Gedupeerden Categorie A, zoals gedefinieerd in **productie A.1)**. Dit betrof in januari 2021 circa 6,5 miljoen personen. Dat het minder personen zijn kan in ieder geval niet aangetoond worden. Een deel van de vorderingen ziet erop om meer helderheid te verkrijgen over de omvang van het GGD-datalek;

b) Personen waarvan vaststaat of zal worden vastgesteld dat hun persoonsgegevens als gevolg van het GGD-datalek door ongeautoriseerde personen zijn ingezien of bij ongeautoriseerde personen in handen zijn gekomen (Gedupeerden Categorie B, zoals gedefinieerd in **productie A.1**).

15. De doelen die Stichting ICAM met deze procedure nastreeft zijn de volgende.

1.2.1 Helderheid over (de omvang en gevolgen van) het GGD-datalek

16. De Gedupeerden hebben belang bij transparantie over het GGD-datalek, de omvang daarvan en de (potentiële) gevolgen voor hun rechten en vrijheden. Momenteel is onduidelijk van hoeveel

Betrokkenen daadwerkelijk gegevens zijn ontvreemd. De Staat c.s. geven daarover onduidelijke en onvolledige informatie en houden belangrijke stukken en informatie achter (paragraaf 3.4). Door de onduidelijke informatievoorziening verkeren miljoenen Gedupeerden in onzekerheid over de vraag of hun persoonsgegevens ontvreemd zijn of niet, of zelfs in de onterechte veronderstelling dat dat niet het geval is. Indien zij juist en volledig geïnformeerd worden over de kans dat hun gegevens in criminele handen terecht zijn gekomen, kunnen zij zich tegen eventueel misbruik van de gegevens beter wapenen. Wanneer duidelijk zou worden dat van bepaalde Gedupeerden daadwerkelijk uitgesloten kan worden dat hun persoonsgegevens zijn ontvreemd, neemt dat hun onzekerheid en daarmee een zware last weg.

17. De incidentele vorderingen sub 10.3 (onderzoek naar de omvang van het datalek), 10.4 (informeren van de Gedupeerden) en 10.5 (het beschikbaar houden van informatie) zijn gericht op dit belang.

1.2.2 Beëindiging van de inbreuk

18. De Gedupeerden hebben belang bij beëindiging van de inbreuk. Volgens de AP voldoen de Staat c.s. namelijk nog altijd niet aan hun (beveiligings)verplichtingen onder de AVG (**producties K.1 en K.26**). De vorderingen sub 11.5 zien erop dat deze inbreuk wordt beëindigd.

1.2.3 Betere beveiliging van IT-systemen en persoonsgegevens door de overheid

19. De Gedupeerden hebben er belang bij dat de overheid ertoe wordt bewogen in zijn algemeenheid een hoger niveau van informatiebeveiliging na te streven. De door Stichting ICAM in deze zaak ingestelde collectieve schadevordering dient mede dit doel.

20. De Nederlandse overheid heeft de afgelopen jaren helaas telkenmale laten zien dat zij niet bereid of in staat is goed om te gaan met de persoonlijke levenssfeer van burgers en hen adequaat te beschermen tegen inbreuken op hun privacy en onrechtmatige verwerking van persoonsgegevens. Voormalig Tweede Kamerlid Verhoeven diende naar aanleiding van het GGD-datalek dan ook een motie in (**productie D.10**):

> "constaterende dat de overheid structureel tekortschiet op AVG-dataveiligheidsprincipes zoals privacy by design, dataminimalisatie, doelbinding en technische en organisatorische voorzieningen, alsmede audits en kwaliteitsnormen"

21. Het is in deze tijd meer dan gerechtvaardigd om overheden, waaronder de Nederlandse overheid, te dwingen passende maatregelen te nemen om het fundamentele recht op gegevensbescherming te waarborgen. De prikkels die daartoe tot heden zijn ingezet zijn kennelijk niet afdoende. Helaas hebben toezichthouders, waaronder de Nederlandse AP, onvoldoende capaciteit om de AVG te handhaven. Daarnaast heeft de AP aangegeven het lastig te vinden om overheden te beboeten omdat die boetes uiteindelijk weer in de schatkist belanden. Ook naar

aanleiding van het GGD-datalek heeft de AP niet handhavend opgetreden. Er is dan ook een publiek belang bij dat de overheid vanuit de maatschappij een sterk signaal krijgt dat zij beter zorg moet dragen voor de beveiliging van persoonsgegevens.

22. Daarbij is ook het gezichtspunt relevant dat burgers persoonsgegevens aan de overheid verstrekken in het vertrouwen dat zij daarmee zorgvuldig om zal gaan. Wanneer de overheid niet zorgvuldig met persoonsgegevens van haar burgers omgaat, bestaat het risico dat burgers de overheid gaan wantrouwen en niet langer bereid zijn gegevens te verstrekken, zoals in dit geval ten behoeve van het testen en vaccineren op corona. Uit representatief onderzoek door KPMG en Motivaction van oktober 2021 blijkt dat privacy-incidenten tijdens de coronacrisis het bewustzijn van Nederlanders hierover hebben vergroot en dat het GGD-datalek een grote impact heeft gehad (**productie K.2**, p. 6):

> "Nederlanders zijn bezorgd over datalekken. Bijna twee derde (63%) is bang dat hierdoor persoonlijke gegevens op straat komen te liggen. Privacyincidenten tijdens de coronacrisis lijken het bewustzijn van de Nederlander te hebben vergroot. Zo blijkt 83% op de hoogte van het grote datalek bij de GGD, dat eind januari 2021 bekend werd. Het administratiesysteem voor het test- en vaccinatieproces en de communicatie hierover werd gehackt en ook werden persoonsgegevens rondom het bron- en contactonderzoek van de GGD buitgemaakt. Privégegevens van miljoenen Nederlanders kwamen hierdoor in handen van kwaadwillenden, die de data via internet doorverkochten.
>
> De impact van dit lek op Nederlanders blijkt behoorlijk groot te zijn geweest", stelt Stephan Idema, die bij KPMG leiding geeft aan het privacyteam. "Zo wilde één op de vijf ondervraagden (22%) zich door het GGD-lek minder snel laten testen op het coronavirus." Deze uitkomst sluit aan bij cijfers van het RIVM. Begin maart maakte het instituut bekend dat 35% van de Nederlanders zich bij klachten liet testen op corona. Begin januari was dat volgens het RIVM nog 50%. Idema: "Deze afname zien we dus terug in de groep van respondenten – één op de vijf – die aangaf
> dat ze na het GGD-lek minder snel een coronatest zouden doen."

23. Bovendien heeft de overheid een belangrijke voorbeeldfunctie waar het gaat om naleving van de AVG en het voldoen aan beveiligingseisen. Als de overheid al zo laks omgaat met de regels, waarom zouden burgers en bedrijven zich daar dan wel aan houden?

24. Bij voorkeur zou Stichting ICAM een vordering instellen die de Staat c.s. verplicht tot het nemen van bepaalde, concreet omschreven verbeteringsmaatregelen. Waarschijnlijk zijn echter Stichting ICAM noch de rechter bevoegd of bij machte om voor te schrijven op welke wijze dat zou moeten gebeuren. Om die reden vordert Stichting ICAM dat niet. Zij meent echter dat toewijzing van een collectieve schadevergoedingsvordering mede het effect zal hebben dat de overheid beter informatiebeveiligingsbeleid implementeert. Naar de overtuiging van Stichting ICAM is civielrechtelijke handhaving middels een collectieve schadevordering een passend middel om verandering te bevorderen. Indien de Staat c.s. ook de (financiële) consequenties van hun optreden ondervinden, mag worden aangenomen dat zij zich ervoor zullen inzetten hun gedrag te verbeteren.

25. De vorderingen sub K (verklaringen voor recht), sub M (immateriële schade) en N (materiële schade) worden mede met het oog op voorgaand belang ingesteld.

1.2.4 Vergoeding van de schade van de Gedupeerden

26. Alle Gedupeerden van het GGD-datalek hebben schade geleden. Die dient te worden vergoed. Dat geldt voor zowel de Gedupeerden Categorie A als de Gedupeerden Categorie B. De Gedupeerden lijden immateriële schade doordat zij de controle over hun persoonsgegevens kwijt zijn. Dat levert bovendien reële gevoelens van onzekerheid, stress en angst op (paragraaf 5.3). Zij moeten continu waakzaam zijn. De Gedupeerden lijden materiële schade doordat zij, voor zover mogelijk, persoonsgegevens moeten (laten) aanpassen en continu moeten controleren of hun gegevens door criminelen niet gebruikt worden om bijvoorbeeld bankgegevens te wijzigen of bestellingen te doen op hun naam (paragraaf 5.4).

27. Ten aanzien van de Gedupeerden Categorie B is niet veel discussie denkbaar dat zij schade hebben geleden: hun gegevens zijn gestolen.

28. Ten aanzien van Gedupeerden Categorie A is een meer principiële discussie denkbaar. Die discussie gaat over de vraag of het feit dat persoonsgegevens zijn gelekt en blootgesteld zijn geweest aan diefstal, reeds schade bij die Gedupeerden veroorzaakt of kan veroorzaken.

29. Stichting ICAM meent van wel. De Gedupeerden Categorie A verkeren immers in onzekerheid over wat er met hun persoonsgegevens is gebeurd of zal gebeuren en of hun gegevens wel of niet gestolen zijn. Doordat de Staat c.s. onvoldoende controlemechanismen hadden geïmplementeerd (paragraaf 3.4 en 4.2.4.4), kunnen zij van geen enkele Gedupeerde uitsluiten dat gegevens zijn gestolen. Feit is dat het datalek en de wetenschap daarvan gevoelens van gemis aan controle en risico op feitelijk misbruik teweeg brengen. Dat is schade, ook als er geen materiële schade wordt toegebracht. Zeker bij een zo ernstig datalek als het GGD-datalek.

30. Een andere opvatting zou ook tot onaanvaardbare gevolgen leiden. Karakteristiek voor schendingen van de AVG is dat ze primair niet tot schade aan zaken leiden, maar tot onjuist behandelen van gegevens. Inherent daaraan is vervolgens dat in veel gevallen (i) niet komt vast te staan of dat tot concrete gevolgen heeft geleid of op enig moment zal leiden, en (ii) als dat wel zo is, causaal verband moeilijk kan worden aangetoond, omdat dezelfde persoonsgegevens ook buit kunnen zijn gemaakt via bijvoorbeeld een ander datalek. De Gedaagden hebben dit verweer ook al gevoerd (paragraaf 7.4).

31. Anders gezegd: voor een Gedupeerde is het vaak onmogelijk om aan te tonen dat een schending van de AVG tot een concreet aan te wijzen gevolg heeft geleid, anders dan de blootstelling of de diefstal zelf. Indien die blootstelling of diefstal geen recht zou geven op schadevergoeding, wordt het recht op schadevergoeding voor AVG-schendingen vrijwel illusoir en daarmee ook de civielrechtelijke handhaving van die normen. Dat is ongewenst. Het heeft bovendien een breder

maatschappelijk gevolg, namelijk dat de goede werking van de AVG onaanvaardbaar zal afnemen. Indien schending van de AVG financieel geen of vrijwel geen gevolgen heeft, zal de prikkel om de AVG na te leven bijzonder laag worden.

32. Wil de AVG doeltreffende waarborgen bieden tegen flagrante schendingen, dan dient deze zodanig te worden uitgelegd dat toekenning van immateriële schadevergoeding de norm is bij ernstige schendingen zoals het GGD-datalek.

33. Er is over dit onderwerp momenteel een aantal procedures aanhangig bij het HvJEU. Stichting ICAM zal deze zaken bespreken in paragraaf 5.2.1.4.

34. De vorderingen sub M (immateriële schade) en N (materiële schade) zijn gericht op beantwoording van voormelde principiële vragen en het verkrijgen van de bedoelde schadevergoeding.

1.3 Omvang van de schade

35. Aan de Gedupeerden Categorie B heeft GGD-koepelorganisatie GGD GHOR een “financieel gebaar” aangeboden van € 500,-, zulks tegen finale kwijting (paragraaf 3.1.12). Dat is onvoldoende. De Staat c.s. miskennen met dat aanbod dat uit de rechtspraak blijkt dat de werkelijke schade bij diefstal van gegevens onder de omstandigheden van deze zaak hoger moet worden begroot dan € 500,-. Voor deze categorie Gedupeerden vordert Stichting ICAM dan ook een bedrag van € 1.500,- aan immateriële schadevergoeding per persoon. De wijze waarop GGD GHOR de finale kwijting heeft geformuleerd biedt hiervoor overigens de ruimte, ook voor de Gedupeerden die het aanbod hebben geaccepteerd (paragraaf 9.1.3.1).

36. De Staat c.s. erkennen dat het feit dat van 1.250 mensen is vastgesteld dat hun gegevens zijn gestolen, niet betekent dat de gegevens van de overige circa 6.498.750 Gedupeerden niet zijn gestolen (Gedupeerden Categorie A) (paragraaf 3.4). Ze stellen enkel dat dat niet is komen vast te staan. Ten aanzien van Gedupeerden Categorie A stellen de Staat c.s. dat geen sprake is van schade. Ze willen die groep dan ook geen schadevergoeding of “financieel gebaar” betalen. Dat is onterecht. De Gedupeerden Categorie A verkeren in onzekerheid over wat er met hun persoonsgegevens is gebeurd en of deze wellicht al zijn misbruikt of in de toekomst nog zullen worden misbruikt. Ook dat levert immateriële schade op, zoals Stichting ICAM nog zal toelichten (paragraaf 5.3). Voor de Gedupeerden Categorie A vordert Stichting ICAM een bedrag van € 500,- aan immateriële schade per persoon.

37. Voor beide categorieën Gedupeerden vordert Stichting ICAM bovendien een bedrag van € 50,- aan materiële schade per persoon (paragraaf 5.4).

38. In totaal komt de vordering van Stichting ICAM uit op een bedrag van € 3.576.250.000,-. Stichting ICAM is zich er vanzelfsprekend van bewust dat toekenning van een schadevordering van deze

omvang een grote impact zal hebben op de rijksbegroting (de minister heeft toegezegd dat de Staat eventuele financiële gevolgen van het GGD-datalek voor de GGD'en zal dragen, **productie D.1B**, p. 19). Dat is echter een gevolg dat voor rekening van de Staat komt en inherent is aan de grote verantwoordelijkheden die hij heeft en de grote budgetten die hem ten dienste staan om die verantwoordelijkheden adequaat in te vullen.

39. Gelet op al het voorgaande is het naar overtuiging van Stichting ICAM van groot belang dat deze zaak door de rechter wordt beoordeeld. Ze wordt in die overtuiging gesteund door bekende privacy-organisaties met wie zij momenteel in overleg is over de vraag of zij hun steun ook publiekelijk willen uitspreken.

1.4 Overleg met gedaagden is niet geslaagd

40. Stichting ICAM heeft getracht om het door haar in deze procedure gevorderde door het voeren van overleg met de Staat c.s. te bereiken. Zij heeft alle Gedaagden schriftelijk uitgenodigd voor overleg, waarop alleen het ministerie, GGD GHOR en de GGD'en zijn ingegaan. Vervolgens is er ook enig overleg geweest, door middel van fysieke besprekingen en schriftelijke correspondentie tussen (de advocaten van) partijen.

41. Helaas heeft dat overleg niet tot een oplossing geleid. De Staat, GGD GHOR en de GGD'en hebben zich met name beroepen op formeel-juridische verweren zoals een beweerd gebrek aan representativiteit en een beweerd gebrek aan causaal verband, althans de onmogelijkheid om causaal verband aan te tonen. Daarnaast hebben zij verwijten geuit in verband met het feit dat deze collectieve procedure extern wordt gefinancierd, waarmee zij echter miskennen dat zonder commerciële procesfinanciers die bereid zijn risico's te nemen, "strooischade" zoals ten gevolge van het GGD-datalek nooit vergoed zou worden. Stichting ICAM verwijst verder naar hetgeen hierover is opgenomen in paragraaf 9.1.1.

1.5 Woo-stukken en Woo-procedures

42. Stichting ICAM heeft bij de Staat, GGD GHOR, de GGD'en, de 25 veiligheidsregio's en bij 25 gemeenten grotendeels gelijkluidende Woo-verzoeken ingediend. In **productiecategorie I** (zie paragraaf 1.7) worden overgelegd de Woo-verzoeken aan de Staat en GGD GHOR en als voorbeeld één Woo-verzoek aan een GGD, één Woo-verzoek aan een Veiligheidsregio en één Woo-verzoek aan een Gemeente:

a) De Staat heeft op de datum van dagvaarding nog niet inhoudelijk gereageerd op het Woo-verzoek van 15 februari 2021 en heeft daarmee de wettelijke termijn van (na verlenging) acht weken ruim overschreden (**productie I.1**). Stichting ICAM zal tegen de weigering om een besluit te nemen in beroep gaan;

b) GGD GHOR heeft zich op het standpunt gesteld dat zij geen bestuursorgaan is en ook anderszins niet verplicht is te voldoen aan Woo-verzoeken (**productie I.2**);

c) De GGD'en hebben nagenoeg allemaal inhoudelijk gereageerd en bepaalde documenten openbaar gemaakt. De documenten waarop Stichting ICAM in deze Dagvaarding een beroep doet, worden overgelegd in **productiecategorie G** (zie paragraaf 1.7).

d) De meeste veiligheidsregio's en gemeenten hebben verwezen naar de GGD'en, sommige hebben wel inhoudelijk gereageerd en documenten openbaar gemaakt.

43. Uit het standpunt van GGD GHOR en uit de door de GGD'en genomen Woo-besluiten blijkt dat de Gedaagden onderling hebben afgestemd dat zij bepaalde documenten niet openbaar zullen maken. Dit betreft vooral documenten die primair bij GGD GHOR zouden berusten, die betrekking hebben op (het gebrek aan) de beveiliging van de GGD-systemen en die waarschijnlijk relevante informatie bevatten over de ernst en omvang van het GGD-datalek. Daarnaast hebben de GGD'en omvangrijke passages zwartgelakt in de documenten die zij wel openbaar hebben gemaakt. Stichting ICAM heeft daarom in een brief van 8 juli 2022 aan de advocaten van GGD GHOR nogmaals verzocht om uiterlijk 25 juli 2022 te voldoen aan haar verplichting tot openbaarmaking op grond van de Woo en haar verzoek om verstrekking van de gevraagde informatie op grond van artikel 843a Rv herhaald (**productie I.2**).

44. Per brief van 22 juli 2022 heeft GGD GHOR gereageerd op het herhaalde Woo-verzoek. Zij blijft, ten onrechte, bij haar standpunt dat zij niet onder het toepassingsbereik van de Woo valt (**productie I.2F**). Per brief van 21 juli 2022 hebben de advocaten van GGD GHOR aan de advocaten van Stichting ICAM laten weten dat GGD GHOR niet zal voldoen aan het verzoek om informatie te verstrekken op grond van artikel 843a Rv (**productie H.2M**).

45. Het beroep dat de GGD'en hebben gedaan op Woo-uitzonderingsgronden voor hun weigering om bepaalde documenten en passages openbaar te maken, is ten aanzien van de meeste van die documenten en passages evident ten onrechte. Stichting ICAM heeft dan ook besloten om tegen vijf Woo-besluiten in bezwaar te gaan. Op de datum van dagvaarding hebben in vier van de vijf bezwaarprocedures hoorzittingen plaatsgevonden en heeft Stichting ICAM van de GGD Zeeland, GGD Drenthe en GGD Rotterdam een beslissing op bezwaar ontvangen. Ook daaruit blijkt dat GGD GHOR en de GGD'en met elkaar hebben afgestemd welke documenten, geheel, geheim moeten blijven. Het betreft een lijst documenten (zie paragraaf 10.2.1) die de GGD'en eerst niet openbaar wilden maken vanwege het belang van het goed functioneren van de Staat (artikel 5.1 lid 2 sub i Woo). Inmiddels heeft GGD Zeeland echter het standpunt ingenomen dat zij deze documenten "bij nader inzien" toch niet "daadwerkelijk" onder zich heeft, kennelijk omdat de DPG Zeeland de documenten alleen onder zich zou hebben in zijn functie als lid van de ledenraad van GGD GHOR. Stichting ICAM is inmiddels in beroep gegaan tegen de beslissing op bezwaar van de GGD Zeeland.

46. De Woo-dossiers worden overlegd in productiecategorie I.

1.6 Incidentele vorderingen

47. Nu de uitkomst van de Woo-procedures nog niet bekend is en de Staat c.s. er alles aan lijken te doen om informatie achter te houden, verzoekt Stichting ICAM de rechtbank om de Staat c.s. te bevelen om bepaalde stukken in het geding te brengen ex artikel 22 Rv en stelt Stichting ICAM een aantal incidentele vorderingen in die erop zijn gericht om duidelijkheid te krijgen over (de omvang en gevolgen van) het GGD-datalek, waaronder een exhibitievordering ex artikel 843a Rv en een vordering tot het bevelen van een deskundigenbericht (zie verder hoofdstuk 10).

1.7 Producties

48. Voor de overzichtelijkheid en in overleg met de griffie van uw rechtbank zijn de producties bij deze Dagvaarding genummerd in verschillende categorieën. Eventuele aanvullende producties zullen binnen deze categorieën worden doorgenummerd:

A. Begrippen en afkortingen
B. Stukken met betrekking tot Stichting ICAM
C. Nieuwsberichten
D. Kamerstukken
E. Literatuur
F. Communicatie vanuit GGD GHOR
G. Woo-stukken
H. Correspondentie met de Gedaagden
I. Woo-correspondentie en Woo-bezwaarschriften
J. Strafvonnissen
K. Overig

49. Veel producties, met name de Woo-stukken, bevatten informatie over verschillende onderwerpen, zoals over toegang en autorisaties, de exportfunctionaliteit en logging. Om de omvang van deze Dagvaarding zoveel mogelijk te beperken, worden deze producties waar mogelijk slechts bij één van de betreffende onderwerpen besproken. Dat heeft tot gevolg dat in bepaalde paragrafen ook bewijs wordt aangedragen en stellingen worden ingenomen over onderwerpen die buiten het bereik van de titel van die paragraaf vallen.

1.8 Definities en afkortingen

50. De in deze Dagvaarding gebruikte begrippen en afkortingen, steeds met een beginhoofdletter geschreven, hebben hierin de betekenis zoals daaraan gegeven in **productie A.1**.

2 PARTIJEN

2.1 Stichting ICAM

51. Stichting ICAM, opgericht op 25 november 2021, is een stichting zonder winstoogmerk. Zij behartigt de belangen van groepen gedupeerden zoals bedoeld in artikel 3:305a BW (massaschade). Eén van haar doelstellingen is optreden tegen (dreigende) inbreuken op het recht op bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens, waaronder inzake inbreuken op deze rechten door de overheid. Haar Statuten vermelden als doel onder andere (**productie B.1)**:

> "(…) 3.1 De Stichting stelt zich ten doel om als onafhankelijke organisatie en zonder winstoogmerk de belangen te behartigen van Gedupeerden, zijnde groepen natuurlijke personen, vennootschappen en/of rechtspersonen, in Nederland en/of daarbuiten, die zijn of dreigen te worden geraakt in een gelijksoortig belang in de zin van artikel 3:305a BW (of een vergelijkbare of daarvoor in de plaats tredende (wettelijke) regeling) en daardoor op enige derde(n) een of meer vordering(en) hebben verband houdend met door deze natuurlijke personen, vennootschappen en/of rechtspersonen geleden of te lijden Massaschade.
>
> 3.2 In het bijzonder valt onder het doel van de Stichting:
> a) Het optreden tegen (dreigende) inbreuken op het recht van burgers, consumenten, vennootschappen en/of rechtspersonen op bescherming van de persoonlijke levenssfeer en bescherming van persoonsgegevens, waaronder in het bijzonder tegen inbreuken door de overheid en/of overheidsinstanties, zoals de Staat en andere publiekrechtelijke rechtspersonen, waaronder begrepen het verhalen van Massaschade die deze Gedupeerden lijden en/of hebben geleden ten gevolge van inbreuken op genoemde rechten, waaronder begrepen overtredingen van de EU Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679) en/of enige daaruit voortvloeiende nationale wet- of regelgeving, beleidsregels, gedragscodes of normen; (…)"

52. Stichting ICAM heeft een Raad van Bestuur en een Raad van Toezicht. De leden van de Raad van Bestuur en de Raad van Toezicht beschikken over de specifieke juridische en financiële deskundigheid en ervaring die noodzakelijk is voor de adequate behartiging van de belangen zoals omschreven in de statuten (paragraaf 9.1.2). Stichting ICAM zal in hoofdstuk 9 toelichten dat zij ontvankelijk is in deze procedure.

2.2 De Staat c.s.

53. Gedaagden in deze procedure zijn:

a) De Staat der Nederlanden (ministerie van Volksgezondheid, Welzijn en Sport);

b) De 25 GGD'en;

c) De vereniging Publieke Gezondheid en Veiligheid Nederland;

d) De stichting Verenigingsbureau Publieke Gezondheid en Veiligheid Nederland;

e) De stichting Projectenbureau Publieke Gezondheid en Veiligheid Nederland;

f) De stichting Landelijke Coördinatie Covid-19 Bestrijding;

g) De Veiligheidsregio Amsterdam-Amstelland;

h) De Veiligheidsregio Rotterdam-Rijnmond;

i) De Gemeente Amsterdam; en

j) De Gemeente Rotterdam.

54. Stichting ICAM heeft de Staat c.s. bij brieven van 8 februari 2022 gesommeerd om bepaalde informatie te bewaren en aan Stichting ICAM te verstrekken, aangekondigd dat zij o.a. vorderingen in zou stellen tot verklaringen voor recht, tot het bevelen het onrechtmatig handelen te staken en tot het informeren van alle Gedupeerden. Ook heeft zij de Staat c.s. aansprakelijk gesteld voor de door de Gedupeerden geleden schade. In de brieven heeft Stichting ICAM de Gedaagden uitgenodigd om in overleg te treden (**productiecategorie H**).[7] Dat overleg heeft plaatsgevonden maar heeft helaas niet geleid tot een oplossing (zie paragraaf 1.4 en 9.1.4.3).

55. In de brieven heeft Stichting ICAM aangegeven dat zij alle betrokken partijen heeft aangeschreven, maar dat zij op basis van nader door hen te verstrekken informatie één of meer partijen eventueel buiten de procedure zou houden indien zou blijken dat zij niet aansprakelijk zijn voor het GGD-datalek. De Staat c.s. hebben echter geen informatie verstrekt op basis waarvan Stichting ICAM deze keuze kon maken. Stichting ICAM is daarom genoodzaakt alle aangeschreven (categorieën van) Gedaagden in deze procedure te betrekken. Voor wat betreft de veiligheidsregio's en de gemeenten heeft Stichting ICAM er om redenen van proces- en kostenefficiëntie voor gekozen per categorie slechts twee partijen aan te spreken. Stichting ICAM stelt zich op het standpunt dat sprake is van hoofdelijke aansprakelijkheid tussen de verwerkingsverantwoordelijken (paragrafen 4.2.1 en 6.4). Indien de gedaagde Veiligheidsregio's en Gemeenten als (gezamenlijk) verwerkingsverantwoordelijken worden aangemerkt, is het aan hen om eventueel regres te nemen op overige veiligheidsregio's en gemeenten.

2.2.1 De Staat der Nederlanden (ministerie van Volksgezondheid, Welzijn en Sport)

56. De Staat der Nederlanden heeft de plicht de volksgezondheid te beschermen. De bestrijding van besmettelijke infectieziekten zoals corona is in dat kader een taak van de Staat. Op grond van

[7] Dit is anders voor de LCCB, die pas later bij Stichting ICAM in beeld kwam en op 22 november 2022 is aangeschreven. De LCCB heeft de brief ter kennisneming aangenomen (**producties H.2N en H.2O**).

artikel 7 lid 1 Wpg geeft de minister dan ook leiding aan de bestrijding van een epidemie van een infectieziekte behorend tot groep A, zoals het coronavirus. Ingevolge dit artikel kan de minister de voorzitters van de veiligheidsregio's instrueren hoe de bestrijding ter hand te nemen, waaronder begrepen het opdragen tot het toepassen van bepaalde maatregelen.

57. Bij de uitbraak van de coronapandemie in Nederland heeft de minister in het kader van zijn taak op grond van artikel 7 lid 1 Wpg de GGD'en gevraagd om - in aanvulling op hun wettelijke taken - het testen en traceren van mensen met klachten die passen bij corona uit te voeren, hoewel de GGD'en niet voorbereid waren op een taak van deze omvang.[8] De Staat heeft daarnaast controlerende zeggenschap gehad over, en actieve bemoeienis gehad bij, de keuze voor en de (door)ontwikkeling, inrichting en ingebruikname van de GGD-systemen. De Staat heeft daartoe specifieke aanwijzingen en instructies gegeven aan de GGD'en en GGD GHOR (paragraaf 4.2.1.1).

2.2.2 De GGD'en

58. De GGD'en zijn openbare lichamen die op grond van artikel 14 lid 1 Wpg door de colleges van burgemeester en wethouders van gemeenten die behoren tot een bepaalde Veiligheidsregio, via het treffen van een gemeenschappelijke regeling zijn ingesteld en in stand worden gehouden. Op grond van artikel 14 lid 5 Wpg kan een GGD ook worden ingesteld en in stand worden gehouden door de colleges van burgemeester en wethouders van de gemeenten in twee of meer veiligheidsregio's. In Nederland zijn in totaal 25 GGD'en. De GGD'en staan onder leiding van een directeur publieke gezondheid, die is benoemd door het algemeen bestuur van de betreffende GGD. Het algemeen bestuur van de GGD bestaat uit vertegenwoordigers van de deelnemende gemeenten. Het algemeen bestuur wijst uit haar midden een dagelijks bestuur aan.

59. De Wpg schrijft voor welke taken de colleges van burgemeester en wethouders aan de GGD'en moeten toewijzen. Deze taken worden landelijk uniform uitgevoerd. Naast de wettelijke taken voert iedere GGD ook aanvullende taken uit voor de betreffende gemeenten (**productie F.2**).

60. Op grond van artikel 6 lid 1 Wpg is één van de wettelijke taken van de colleges de uitvoering van de algemene infectieziektebestrijding, welke taak zij hebben toegewezen aan de GGD'en. Het testen op corona en het uitvoeren van bron- en contactonderzoek (BCO) valt daar echter niet onder. De minister heeft, zoals aangegeven, de GGD´en echter gevraagd om in aanvulling op hun wettelijke taken het testen en traceren van mensen met klachten die passen bij corona uit te voeren.

[8] *Kamerstukken II* 2020-2021, 27 529, nr. 235, p. 6 (**productie D.3**).

2.2.3 GGD GHOR

61. GGD GHOR is de brancheorganisatie van de 25 GGD'en en de Geneeskundige Hulpverleningsorganisaties in de Regio (GHOR). GGD GHOR omschrijft zichzelf onder andere als de verbindende schakel met ministeries en andere partners (**productie F.1**).

62. GGD GHOR is opgericht als de Vereniging Publieke Gezondheid en Veiligheid Nederland. De activiteiten van de vereniging zijn ondergebracht in de stichting Verenigingsbureau Publieke Gezondheid en Veiligheid Nederland en de stichting Projectenbureau Publieke Gezondheid en Veiligheid Nederland, die worden aangestuurd door het bestuur van de vereniging. Naast voornoemde stichtingen is per 1 januari 2022 de stichting Landelijke Coördinatie Covid-19 Bestrijding (LCCB) opgericht. In deze stichting zijn de activiteiten van GGD GHOR op het gebied van coronabestrijding ondergebracht.

63. GGD GHOR had gedurende de bestrijding van de coronapandemie een sleutelrol in de aansturing van de GGD'en en in het contact tussen de GGD'en en het ministerie. Ook bij de inrichting van de IT-systemen had GGD GHOR een cruciale rol. Zo blijkt uit een Kamerbrief van 2 februari 2021 dat het GGD GHOR was die heeft besloten tot het beperken van de groep die gebruik kan maken van HPZone.[9] Dit illustreert bij uitstek dat GGD GHOR niet alleen aanspreekpunt is, maar dat zij een besluitvormende sleutelrol op zich neemt.

2.2.4 De Veiligheidsregio's

64. De Veiligheidsregio's zijn openbare lichamen die op grond van artikel 9 van de Wet veiligheidsregio's ("**Wvr**") door de colleges van burgemeester en wethouders van de gemeenten die behoren tot een bepaalde regio, via het treffen van een gemeenschappelijke regeling zijn ingesteld en in stand worden gehouden. Nederland is verdeeld in 25 veiligheidsregio's. Iedere Veiligheidsregio zet zich in voor de veiligheid van de inwoners en bezoekers van dat gebied. Het bestuur van een Veiligheidsregio bestaat uit de burgemeesters uit die regio. Een van die burgemeesters wordt bij Koninklijk Besluit benoemd tot voorzitter, meestal de burgemeester van de grootste gemeente. Op dezelfde dag dat landelijke coronamaatregelen werden afgekondigd, 12 maart 2020, werden alle veiligheidsregio's opgeschaald naar GRIP-4 (ramp waarbij meerdere gemeenten betrokken zijn) en werd artikel 39 Wvr van toepassing verklaard. Daarmee gingen verschillende bevoegdheden die verband houden met de openbare orde en veiligheid van rechtswege over naar de voorzitters van de veiligheidsregio's. Het gaat daarbij op grond van artikel 7 Wvr onder meer om het informeren "over de oorsprong, de omvang en de gevolgen van een ramp of crisis die de gemeente bedreigt of treft, alsmede over de daarbij te volgen gedragslijn". Vanaf 1 december 2020 verving de Tijdelijke wet maatregelen covid-19 ("**Twm**") artikel 39 Wvr als basis voor de maatregelen die werden genomen, waarmee de bestuurlijke verantwoordelijkheid voor de handhaving van de coronamaatregelen weer bij de burgemeesters

[9] *Kamerstukken II* 2020-2021, 27 529, nr. 235, p. 1 (**productie D.3**).

kwam te liggen. De verantwoordelijkheden en bevoegdheden van de voorzitters van de veiligheidsregio's op grond van de Wpg bleven echter onverminderd van kracht.

65. 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. Overeenkomstig het vierde lid moet de voorzitter van de Veiligheidsregio zorg dragen voor de bestrijding zelf. Verder kan de minister de voorzitters van de veiligheidsregio's op grond van artikel 7 Wpg instructies geven hoe de bestrijding ter hand te nemen.

2.2.5 De Gemeenten

66. De colleges van burgemeester en wethouders van de Nederlandse gemeenten zijn op grond van de Wpg belast met het uitvoeren van taken ter bevordering en continuering van de publieke gezondheidszorg. 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. De colleges zorgen verder voor de instelling en instandhouding van de GGD´en aan wie zij taken op grond van de Wpg uitbesteden. Gemeenten financieren de GGD´en, houden toezicht en zijn eindverantwoordelijk.

3 FEITEN

3.1 Chronologisch overzicht

3.1.1 Eerste aanwijzingen van het GGD-datalek

67. Op 16 september 2020 meldde actualiteitenprogramma Nieuwsuur dat callcentermedewerkers die voor de GGD'en coronatestafspraken inplannen en mensen op de hoogte brengen van negatieve testuitslagen, toegang hadden tot persoonsgegevens waartoe zij voor die doeleinden geen toegang hoefden te hebben (**productie C.1**).

68. Op dezelfde datum meldde RTV Oost dat het account van een GGD-callcentermedewerker die slechts twee dagen voor de coronatestlijn had gewerkt, een maand na uitdiensttreding nog altijd toegang gaf tot alle gegevens van mensen die zich op corona hadden laten testen. De medewerker gaf aan dat hij volledige toegang kreeg, nog voordat hij een Verklaring het Gedrag (VOG) had ingeleverd (**productie C.2**).

69. Uit een artikel in dagblad Trouw van 9 oktober 2020 blijkt dat de AP naar aanleiding van de publicatie door RTV Oost vragen heeft gesteld aan GGD GHOR. Uit intern onderzoek van Teleperformance – het Franse callcenterbedrijf aan wie de coronatestlijn was uitbesteed – zou

zijn gebleken dat bij in ieder geval 37 andere uitzendkrachten soortgelijke fouten waren gemaakt. Van dit datalek werd een melding gedaan bij de AP (**productie C.3**). Uit de beantwoording van Kamervragen door de minister blijkt dat de GGD'en door de AP uitdrukkelijk zijn gewezen op hun wettelijke verplichting te zorgen dat gegevens van burgers goed beveiligd zijn. De AP zou daarbij hebben aangegeven dat de GGD'en risico's in kaart moesten brengen en waar nodig maatregelen moesten treffen om bestaande (en toekomstige) problemen op te lossen.[10]

70. Op 3 november 2020 berichtte het Algemeen Dagblad over een incident dat aan het licht kwam nadat een tipgever via klokkenluidersplatform Publeaks een melding deed van misbruik van CoronIT. GGD-medewerkers hebben ongeoorloofd dossiers ingezien van bekende Nederlanders die een coronatest hadden gedaan. Als bewijs werden screenshots van de gegevens van twee personen in het systeem getoond, waaronder gegevens van de Rotterdamse burgemeester Achmed Aboutaleb, die onder voortdurende politiebescherming staat. Ook kwam het voor dat medewerkers telefoonnummers uitwisselden van "knappe mannen en vrouwen" die zich hadden laten testen. GGD HOR reageerde dat het "niet wenselijk [is] om toegang tot de gegevens voor medewerkers te beperken. GGD-medewerkers moeten alle dossiers kunnen inzien om hun werkzaamheden voor alle 25 GGD'en goed uit te kunnen voeren." (**productie C.4**).

71. Op 12 november 2020 meldde de Volkskrant dat GGD GHOR er al in juni 2020 mee bekend was dat HPZone niet geschikt was voor gebruik in grootschalige epidemieën. Ook de maker van deze software zou dit reeds hebben bevestigd (**productie C.5**). Niet alleen nieuwsbronnen bevestigen dat HPZone niet geschikt was voor het verwerken van gegevens in deze omvang, GGD GHOR heeft dat zelf toegegeven in haar reactie van 29 januari 2021 (**productie F.3**).

3.1.2 Risicoanalyses van de getroffen systemen

72. Uit notulen van een stuurgroepvergadering van de Landelijke Coördinatiestructuur Testcapaciteit van 17 december 2020 volgt dat zowel GGD GHOR als het ministerie naar aanleiding van risicoanalyses door KPMG en de Regiegroep DOTT (een in opdracht van de minister opgerichte regiegroep voor Digitale Ondersteuning van de Test- en Traceerketen) toen al op de hoogte waren van "serieuze kwetsbaarheden" in de IT-systemen (**productie D.5**).

73. De minister informeerde de Tweede Kamer op 24 december 2020 over de "risicoanalyse van de digitale testketen", die in opdracht van het ministerie, GGD GHOR en het RIVM was uitgevoerd. De risicoanalyse had kwetsbaarheden blootgelegd, onder meer op het gebied van informatiebeveiliging. De risicoanalyse werd op 11 december 2020 in concept opgeleverd, maar is ''vanwege veiligheidsredenen'' niet openbaar gemaakt. De minister gaf in een Kamerbrief aan

[10] *Kamerstukken II* 2020/21, 27 529 en 32 761, nr. 234 (*Verslag van een schriftelijk overleg*), p. 68, vraag 359 (**productie D.2**).

dat hij naar aanleiding van de risicoanalyse samen met de ketenpartners onder andere de volgende maatregelen zou nemen om de risico's te beheersen:[11]

a) Om het risico op datalekken te minimaliseren zou een beter passend autorisatiebeheer worden ingericht. Hierdoor zou het voor onbevoegde en/of niet-geautoriseerde gebruikers onmogelijk worden gemaakt om toegang te krijgen tot bepaalde gegevens;

b) Er zou hoogwaardige cybersecurity expertise worden ingezet in om de beveiliging van het systeemlandschap te verbeteren en kwetsbaarheden verder uit te sluiten (met name op het gebied van informatiebeveiliging en bescherming van persoonsgegevens);

c) De minister zou de Regiegroep DOTT opdracht geven om samen met de ketenpartners een laagdrempelig incidentproces te formaliseren, zodat de partijen eerder in gezamenlijkheid op de hoogte zouden zijn van incidenten en andere verstoringen, en daar beter en sneller op zouden kunnen reageren.

74. De risicoanalyses bevatten aldus waarschijnlijk relevante informatie over de beveiligingsmaatregelen en kwetsbaarheden in de GGD-systemen.

3.1.3 Berichtgeving door RTL Nieuws en NOS

75. Op 25 januari 2021 berichtte RTL Nieuws dat op chatdiensten als Telegram, Snapchat en Wickr tientallen accounts waren aangetroffen die al maandenlang persoonsgegevens te koop aanboden, afkomstig uit zowel CoronIT als HP Zone Lite. Er zou grootschalig worden gehandeld in miljoenen adresgegevens, telefoonnummers en BSNs. Sommige accounts zouden grote datasets aanbieden met daarin de gegevens van vele tienduizenden personen.

76. RTL Nieuws vroeg bij de handelaren gegevens op van een aantal personen en in alle gevallen ontving zij het juiste woonadres, telefoonnummer, e-mailadres en BSN. Ook heeft RTL Nieuws een dataset ingezien van honderden Nederlanders, illegaal verkregen uit HP Zone Lite. Deze dataset was volgens de aanbieder een voorproefje van de vele duizenden tot tienduizenden personen van wie hij persoonsgegevens kon aanleveren. Er werden zelfs specifieke datasets op aanvraag geleverd, bijvoorbeeld alleen mensen uit Amsterdam of enkel vijftigplussers. Eén van de verkopers zei dat er veel vraag was naar de gegevens. "Ik eet goed broer", vertelde hij in een chatgesprek, ernaar verwijzend dat hij veel geld verdiende met de verkoop van de data. De AP reageerde op vragen van RTL Nieuws dat "Dit zeer kwalijk [is] en mogelijk een ernstig datalek […]. De AP heeft de GGD direct om opheldering geëist. Deze data bevatten naam, adres, woonplaats en telefoonnummers en ook nog eens BSN's: allemaal actueel en in grote hoeveelheden. Dat is heel veel waard." De AP gaf aan dat een organisatie nalatig kan zijn als het de gegevens in zijn

[11] *Kamerstukken II*, 2020-2021, 25 295, nr. 843, p. 4 e.v. (**productie D.5**).

systemen niet voldoende beveiligt: "Dan riskeer je niet alleen een boete van de AP, maar ook bijvoorbeeld massaclaims van slachtoffers." (**productie C.6**).

77. Op 28 januari 2021 meldde RTL Nieuws dat zij tientallen GGD-medewerkers had gesproken (**productie C.8**). Uit die gesprekken bleek dat onder andere de organisatorische beveiligingsmaatregelen tekortschoten:

a) Ten eerste bleek uit de gesprekken dat de GGD-medewerkers te ruime toegang hadden tot gegevens: ““Ik heb toegang tot de gegevens uit de coronasystemen van allerlei andere GGD-regio’s waar ik helemaal geen toegang tot zou moeten hebben”, vertelt een werknemer die via een derde partij voor de GGD werkt. “Iedereen zoekt vrienden, familie of bekende mensen op en met de exportknop kon je er tot voor kort alle gegevens uit halen. Het verbaast me niets dat er wordt gehandeld in die privégegevens.”” en ““Bij de instructie van CoronIT werd ook nadrukkelijk gezegd dat je overal bij kunt en of je daar alsjeblieft geen misbruik van wil maken. En het erge is: ik heb voor mijn werk helemaal geen toegang tot die data nodig, maar ik kon echt overal bij.””;

b) Ten tweede bleek dat de medewerkers vaak zonder VOG aan het werk waren: “Meer dan tien medewerkers die RTL Nieuws sprak hebben nooit een VOG ingeleverd of pas maanden nadat zij al aan de slag waren. Opvallend genoeg kreeg een aantal van hen deze week opeens de vraag of ze toch nog een VOG konden inleveren.” en ““Ik heb een sollicitatie van twee minuten gehad, nooit een VOG ingeleverd en mocht gelijk beginnen””;

c) Ten derde bleek dat er onvoldoende toezicht was op het aanmaken van accounts voor de GGD-systemen: ““Ik heb tientallen keren een account laten aanmaken zonder enige controle […]””; en

d) Ten vierde bleek dat er nauwelijks serieuze controles plaatsvonden: “Enkele werknemers vertellen hoe ze eens in de zoveel maanden hun scherm via Microsoft Teams moeten delen om vervolgens de digitale prullenbak te openen. De manager kijkt dan of daar gestolen gegevens uit de coronasystemen in te vinden waren. “Een wassen neus”, wordt het genoemd.”.

78. Ook meldde RTL Nieuws dat de GGD al maanden op de hoogte was van de beveiligingsrisico’s, maar niets had gedaan om de kwetsbaarheden aan te pakken. Daarbij was interne kritiek genegeerd. RTL Nieuws sprak medewerkers die aangaven dat in ieder geval in de zomer van 2020 al interne meldingen waren gedaan.

79. De NOS berichtte op 28 januari 2021 dat het lek in de GGD-systemen al driekwart jaar aanwezig was. Voor medewerkers en extern personeel van de GGD’en was het al sinds de start van het corona-testsysteem mogelijk om met gebruik van de exportfunctie lijsten met geteste mensen

uit te printen. Ook bevatte CoronIT al sinds het begin van de coronapandemie de mogelijkheid om binnen het systeem op een bepaalde persoon te zoeken. Binnen HPZone Lite bestond deze zoekfunctie ook, zo berichtte de NOS. Medewerkers van de GGD konden bij alle dossiers, ook bij dossiers die zij niet toebedeeld hadden gekregen (**productie C.9**).

3.1.4 De eerste reactie van GGD GHOR

80. GGD GHOR-voorzitter André Rouwvoet gaf kort na de berichtgeving door RTL Nieuws en de NOS aan dat GGD GHOR al vanaf het begin van de coronapandemie wist dat haar systemen kwetsbaar waren. Hij verklaarde op 29 januari 2021 aan RTL Nieuws het volgende (**productie C.10**):

> "Dat het registratiesysteem van de GGD niet veilig is, was bekend. Dat zegt Andre Rouvoet, voorzitter van de landelijke koepel GGD GHOR Nederland. "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", zegt Rouvoet over het lekken van persoonsgegevens uit het GGD-systeem. "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."
> De GGD-voorzitter stelt dat onder druk van het coronavirus gekozen is om het computersysteem toch te blijven gebruiken. "Tijdens de tweede golf hebben we besloten om door te gaan met dit systeem, om snel te kunnen blijven werken. Dat was een verkeerde keuze, want het was niet veilig genoeg te maken."

81. Op 12 februari 2021 plaatste GGD GHOR naar aanleiding van het datalek een bericht op haar website waarin zij aangaf hoe betrokkenen een verzoek tot verwijdering van hun gegevens konden doen (**productie F.4**). Op 23 februari 2021 volgde een bericht met "Veelgestelde vragen over het datalek". Dit bericht is daarna meerdere keren geüpdatet (**producties F.5 t/m F.15**). Op de inhoud van deze berichten wordt in de volgende hoofdstukken verder ingegaan.

3.1.5 GGD'en onder verscherpt toezicht van de AP

82. Naar aanleiding van de berichtgeving van Nieuwsuur van 16 september 2020 (randnummer 67) had de AP de GGD'en al uitdrukkelijk gewezen op hun wettelijke verplichting ervoor te zorgen dat de gegevens van betrokkenen goed beveiligd zijn. De AP gaf daarbij aan dat de GGD'en risico's in kaart moesten brengen en waar nodig maatregelen moesten treffen om bestaande (en toekomstige) problemen op te lossen. In november 2020 nam de AP wederom contact op met de GGD'en, ditmaal in verband met het datalek waarover het Algemeen Dagblad had bericht op 3 november 2020 (randnummer 70). De AP stelde vragen en GGD GHOR kondigde maatregelen

aan, die eind 2020/begin 2021 ingevoerd zouden worden **(productie C.3**). Na de onthullingen door RTL Nieuws in januari 2021 verscherpte de AP het toezicht op de GGD'en (**productie C.11**).[12]

3.1.6 Kamerdebat

83. Op 29 januari 2021 zijn door de Tweede Kamer een groot aantal schriftelijke vragen gesteld, die op 2 februari zijn beantwoord (**productie D.2**). Het merendeel van de vragen zag op de vraag hoe het GGD-datalek heeft kunnen plaatsvinden. Zo werd onder meer gevraagd naar hoe GGD-medewerkers gescreend werden, hoe de toegang tot de (functionaliteiten in de) systemen door medewerkers was ingericht, welke andere (beveiligings)maatregelen genomen waren en wat de gevolgen van het datalek konden zijn. Voor wat betreft de omvang en de feitelijke gang van zaken verwees de minister naar het politieonderzoek, dat ten tijde van de beantwoording van de vragen nog niet afgerond was. Voor het overige verwees de minister voornamelijk naar wat GGD GHOR hem had medegedeeld over het datalek. Enkele van de belangrijkste conclusies waren dat de screening niet altijd volledig was afgerond voordat medewerkers aan het werk gingen, dat de toekenning van rechten aan medewerkers te ruim was, dat de logging tekortschoot en dat de controle daarvan niet geautomatiseerd maar slechts steekproefsgewijs plaatsvond.

84. Op 2 februari 2021 voorzag de minister de Tweede Kamer in een Kamerbrief van de laatste stand van zaken (**productie D.3**). De minister opent door op te merken dat mensen er te allen tijde op moeten kunnen vertrouwen dat medische gegevens veilig worden gedeeld en bewaard, juist nu deze gegevens privacygevoelig van karakter zijn. Het GGD-datalek noemt hij dan ook betreurenswaardig en zeer ernstig. In de Kamerbrief erkent de minister onder meer dat de GGD'en niet voldeden aan de laatste NEN-normen en dat de toegang tot print- en exportfuncties in de systemen niet beperkt was tot de medewerkers die deze functies daadwerkelijk nodig hadden voor hun werkzaamheden. Logbestanden werden niet geautomatiseerd gecontroleerd. Ten aanzien van de screening van GGD-medewerkers beschrijft de minister verschillende voorzorgsmaatregelen die genomen werden, zoals het laten tekenen van een geheimhoudingsverklaring en het vragen van een VOG, maar geeft hij ook aan dat het mogelijk was om in afwachting van een VOG al aan het werk te gaan bij een GGD. De focus lag op de functionaliteit van de systemen, maar naar bleek onvoldoende op privacy en datagevoeligheid, zo schrijft de minister. In een kort feitenrelaas bespreekt de minister onder meer dat al eerder, namelijk in september 2020, signalen bestonden dat GGD-medewerkers inzage hadden in alle persoonsgegevens die in de systemen waren opgeslagen.

85. Op 3 februari 2021 vond een Kamerdebat plaats. In de kern ging het debat over de vraag hoe het GGD-datalek heeft kunnen plaatsvinden, welke signalen er al bestonden en wat er moest gebeuren om verdere diefstal van gegevens te voorkomen. Andere belangrijke zaken die aan de

[12] Zie ook *Kamerstukken II* 2020/21, 27 529 en 32 761, nr. 234 (*Verslag van een schriftelijk overleg*), p. 66, vraag 349 (**productie D.2**).

orde kwamen waren de slachtoffers van het datalek en het herstel van het vertrouwen van burgers.[13]

86. Tijdens het debat verweten verschillende Kamerleden de minister dat hij misplaatst reageerde op het datalek, met “volstrekte onderschatting” van het probleem en het gemakzuchtig wegwuiven van zorgen:

> “Mevrouw **Kröger** (GroenLinks):
> […]
> "Ja, jongens, zo werkt het nu eenmaal." Dat was de reactie van de minister tijdens het vragenuurtje vorige week, toen mijn collega Buitenweg aandrong op een antwoord op de vraag of het klopte dat duizenden medewerkers — we begrijpen nu uit de brieven dat het om tienduizenden medewerkers gaat — toegang hebben tot gevoelige informatie van miljoenen Nederlanders. "Zo werkt het nu een maal." Die houding is wat ons betreft precies het probleem, want zo hoeft het natuurlijk helemaal niet te werken, als je privacy by design als uitgangspunt neemt en als je basisprincipe bij het ontwerp van al je IT-systemen is dat zo min mogelijk medewerkers toegang hebben tot zo min mogelijk informatie om het werk toch goed te kunnen blijven doen. Want waarom zou een callcentermedewerker alle mensen die getest worden op moeten kunnen zoeken? Waarom zou iemand die bron- en contactonderzoek doet en dus mensen belt met de vraag met wie ze contact hebben, ook de gegevens van 100 mensen moeten kunnen uitprinten of downloaden? Dat is onnodig en risicovol.”[14]

87. Bovendien uitten Kamerleden hun zorgen over het beschadigde vertrouwen van burgers in hoe de overheid met hun gegevens omgaat en de mogelijke gevolgen die dat kan hebben voor de bestrijding van de coronapandemie. Bovendien lopen burgers grote risico’s, nu hun gegevens voor tienduizenden medewerkers van de GGD’en inzichtelijk waren:

> “Mevrouw **Agema** (PVV):
> Een open deur roept den dief" is een spreuk van de bekende Nederlandse dichter en politicus Jacob Cats uit 1632. Hoe toepasselijk in de kwestie die wij hier vandaag bespreken en hoe jammer dat deze spreuk niet gebeiteld staat in de gevel van het Catshuis, waar het kabinet met enige regelmaat de coronaplannen bespreekt. Want zo is het toch in feite? Binnen het systeem voor het testbeleid stonden alle deuren wagenwijd open. Geen deur zat op slot. Je hoefde zelfs niet aan te kloppen. Iedereen kon overal naar binnen. Niemand controleerde wie er in- of uitging en wat er meegenomen werd. Zo kon het gebeuren dat dieven maandenlang hun gang konden gaan.
> Wat betekent het als je identiteit gestolen wordt? De dief verpatst je identiteit voor een paar tientjes en criminelen bestellen vervolgens spullen op jouw naam, vragen in jouw naam een toeslag aan, sluiten in jouw naam abonnementen af of troggelen je geld af via jouw whatsapp. […]”[15]

---

13 *Handelingen II* 2020/21, nr. 52, item 3 en item 6 (*Privacylek in de systemen van de GGD, gecorrigeerd stenogram)* (**producties D.1A en D.1B**).

14 *Handelingen II* 2020/21, nr. 52, item 3 (*Privacylek in de systemen van de GGD, gecorrigeerd stenogram)*, p. 4 (**productie D.1A**).

15 *Handelingen II* 2020/21, nr. 52, item 3 (*Privacylek in de systemen van de GGD, gecorrigeerd stenogram)*, p. 13 (**productie D.1A**).

88. In de tweede termijn van het debat zette de minister een aantal zaken recht waarover hij de Kamer onjuist, dan wel niet nauwkeurig, geïnformeerd had. Zo had de minister tegen de Kamer gezegd dat "tegen een misdrijf geen kruid gewassen is":

> "Tot slot mijn uitspraak — ik denk eerlijk gezegd dat die nog het meest steekt bij Kamerleden, en zo heb ik u ook gehoord in de eerste termijn — dat tegen een misdrijf, een misdaad, geen kruid gewassen is. Nu ik in de afgelopen dagen alles goed op een rij heb gezet, wat er wanneer bekend was, wat er aan voorgenomen acties wel is uitgevoerd en nog niet is uitgevoerd, moet je op z'n minst zeggen: er was wel meer kruid tegen gewassen geweest. Zoals de voorzitter van de GGD zelf ook zei: gelegenheid maakt de dief. Mevrouw Agema had een citaat van Jacob Cats. Misschien had ik dat citaat daar ook bij moeten gebruiken, want inderdaad, als je de gelegenheid zo duidelijk biedt, dan is het nog steeds een misdrijf, en uiteindelijk is tegen een misdrijf ook geen kruid gewassen, maar hier was wel veel meer kruid tegen gewassen geweest. Ik hecht eraan om dat voorafgaand aan het debat recht te zetten in de richting van uw Kamer, voorzitter."[16]

89. Bovendien erkende de minister dat er al eerder signalen waren dat medewerkers mensen konden opzoeken in de GGD-systemen. Daarbij gaf de minister aan dat de systemen "natuurlijk niet allemaal vanaf het begin fit for purpose waren". Dat maakte dan ook dat de minister eind 2020 opdracht had gegeven voor een risicoanalyse. Volgens de minister bevatte het signaal van RTL Nieuws vergelijkbare observaties als die al uit de risicoanalyse waren gebleken.

90. In gesprekken met de GGD'en was volgens de minister voornamelijk de snelheid van de systemen onderwerp van gesprek, privacy was daarbij een onderbelicht thema:

> "Ja, dat is zo. Dat is zeker zo. Dat geldt voor die twee systemen natuurlijk enigszins verschillend. Bij HPZone kun je zeggen dat dat in de oorsprong — dat systeem is in 2003 ontwikkeld en wordt door bijna alle GGD'en gebruikt — nooit bedoeld is geweest voor dit type gebruik. HPZone is bedoeld geweest voor een exquise club van artsen infectie- ziektebestrijding, een kleine club die daarvan gebruikmaakt, met alle waarborgen van dien. Het is nooit bedoeld voor duizenden bron- en contactonderzoekers, ook van buiten, die in het systeem zouden kunnen. Daarvoor is het systeem überhaupt niet geschikt geweest. Bij CoronIT is er wel degelijk, ook vanaf het begin, aandacht geweest voor privacy. Ik zeg niet dat het een uitruil is tussen het een of het ander. Ik zeg ook niet dat het een tegenstelling is. Ik zeg wel het volgende. Als ik terugkijk naar waarover het departement met de GGD het meest heeft gesproken met betrekking tot CoronIT of überhaupt testen en traceren, dan was dat over: kan het sneller, kan er meer, kan het beter et cetera? Dat was dus veel meer de inhoud van het gesprek dan de privacy."[17]

91. De minister gaf daarbij aan dat hij als opdrachtgever van GGD GHOR en de GGD'en betere en eerdere opvolging had moeten geven aan de ontvangen signalen en de acties die daarop wel en niet waren genomen.

---

16 *Handelingen II* 2020/21, nr. 52, item 6 (*Privacylek in de systemen van de GGD, gecorrigeerd stenogram)*, p. 4 (**productie D.1B**).

17 *Handelingen II* 2020/21, nr. 52, item 6 (*Privacylek in de systemen van de GGD, gecorrigeerd stenogram)*, p. 6 (**productie D.1B**).

92. In het debat gaf de minister aan dat over de omvang van het datalek nog weinig concreets kon worden gezegd, nu dat zou moeten blijken uit het politieonderzoek. De minister gaf wel aan dat de GGD'en aansprakelijk zijn voor schade die voortvloeit uit het datalek, waar nodig met ondersteuning van het ministerie van VWS:

> "Er is ook gevraagd: zou je dan ook kunnen compenseren? Ik dacht dat 50PLUS dat gevraagd heeft, maar ook de VVD, de SGP, het CDA en de PVV. Wie compenseert de schade en zorgt er voor juridische bijstand? De GGD is natuurlijk aan zet, want het is gewoon wettelijk verplicht om te informeren. Maar als er sprake is van schade die zou voortvloeien uit het datalek, is de GGD daar op dat moment ook voor aansprakelijk. En als de GGD daarbij ondersteuning nodig heeft vanuit VWS, zal ik die natuurlijk geven. Dus in formele zin is het de GGD, maar als er sprake zou zijn van noodzaak tot ondersteuning, zullen we dat natuurlijk doen."[18]

93. In deze Dagvaarding zal voor de feitelijke onderbouwing van de vorderingen van Stichting ICAM onder meer worden verwezen naar hetgeen de minister – op basis van informatie van GGD GHOR – in de verschillende Kamerstukken heeft verklaard.

3.1.7 Tweede Kamermoties

94. Naar aanleiding van het Kamerdebat zijn door verschillende Kamerleden moties ingediend (**productie D.10**).

95. Van Brenk c.s. wezen erop dat criminelen misbruik kunnen maken van de gegevens die gelekt zijn uit de systemen van de GGD. Zo kunnen zij onder meer leningen en telefoonabonnementen afsluiten met deze gegevens. Dat kan veel financiële en persoonlijke schade aanrichten bij de betrokkenen. Het was volgens van Brenk c.s. voor criminelen "kinderlijk eenvoudig" om de persoonsgegevens van grote groepen mensen te verkrijgen door de slechte ICT-inrichting. De overheid is door die inrichting dan ook medeverantwoordelijk voor de veroorzaakte schade en moet alles op alles zetten om de geleden schade te vergoeden.

96. Kröger c.s. benadrukten dat tekortkomingen in de systemen van de GGD aan de basis liggen van dit omvangrijke lek van gevoelige persoonsgegevens. Privacy-by-design was wel een uitgangspunt dat aan de ontwikkelaar van het systeem CoronIT was meegegeven, maar toch voldeed het systeem niet aan de privacy-by-designnormen. Kröger c.s. verzochten de regering dan ook om een duidelijk pakket van eisen samen te stellen met betrekking tot deze normen, dat publieke en semipublieke organisaties kunnen gebruiken bij aanbestedingen van hun digitale systemen. Zo moet ervoor worden gezorgd dat deze principes ook echt centraal staan.

[18] *Handelingen II* 2020/21, nr. 52, item 6 (*Privacylek in de systemen van de GGD, gecorrigeerd stenogram)*, p. 19 (**productie D.1B**).

97. Van Esch onderstreepte dat GGD GHOR niet voldoet aan NEN 7510, de staande norm voor informatiebeveiliging in de zorg, en dat de zorgsector al jarenlang de sector is met de meeste datalekken en ICT-systemen structureel niet op orde blijken.

98. Agema gaf aan dat het datalek terecht voor zorgen, onrust en wantrouwen zorgt bij de bevolking. Ten tijde van de motie hadden zich al 40 mensen gemeld bij de Fraudehelpdesk inzake het GGD-datalek. Agema verzocht de regering met een plan te komen om dataschade te voorkomen en herstellen.

99. Tot slot wezen Van den Berg c.s. erop dat het datalek bij de GGD duidelijk maakte dat GGD GHOR het ICT-beleid niet op orde heeft. Er bleek geen centraal geleide ICT-aanpak bij de GGD'en te zijn.

3.1.8 Onderzoek door GGD GHOR en de politie

100. GGD GHOR heeft door cybersecuritybedrijf Fox-IT onderzoek laten uitvoeren naar het GGD-datalek. Hoewel de bevindingen in het rapport van Fox-IT waarschijnlijk van groot belang zijn voor het vaststellen van de ernst en omvang van het GGD-datalek, en daarmee voor de Gedupeerden en voor de maatschappij als geheel, is het rapport niet openbaar gemaakt of aan Stichting ICAM c.s. verstrekt, ondanks herhaalde verzoeken daartoe.

101. GGD GHOR heeft op 22 januari 2021 bij de politie aangifte gedaan van de datadiefstal uit de GGD-systemen, nadat haar bekend werd dat op Telegram persoonsgegevens uit de GGD-systemen verkocht werden. Het cybercrimeteam van de politie Midden-Nederland heeft na de aangifte van GGD GHOR een onderzoek ingesteld. Dat leidde een dag later tot de aanhouding van twee verdachten en uiteindelijk zijn er in totaal acht verdachten aangehouden, zo berichtte GGD GHOR op 5 april 2022 (**productie F.19**). De gepubliceerde strafvonnissen worden overgelegd als **producties J.1 tot en met J.5**.

102. Aanvankelijk liet GGD GHOR op 19 maart 2021 weten dat uit het politieonderzoek was gebleken dat de persoonsgegevens van ongeveer 1.000 personen daadwerkelijk online te koop waren aangeboden (**productie F.10**). Bijna vier maanden later stelde GGD GHOR dit aantal bij naar circa 1.250. Deze mensen zouden allemaal een excuusbrief van de GGD hebben ontvangen (**productie F.14 en F.20)**. Zij kondigde aan een financieel gebaar richting deze gedupeerden te willen maken (paragraaf 3.1.12).

3.1.9 Onderzoek Autoriteit Persoonsgegevens

103. Naar aanleiding van het GGD-datalek heeft de AP aangekondigd het toezicht op de GGD'en te intensiveren en heeft zij onderzoek gedaan. De AP heeft onderzocht of door GGD GHOR en twee onderzochte GGD'en passende technische en organisatorische maatregelen waren getroffen om de persoonsgegevens die worden verwerkt in het kader van het testen, vaccineren en BCO passend te beveiligen. In het onderzoek van de AP, waarover op 8 november 2021 een brief is

gestuurd naar GGD GHOR en de GGD'en, is vastgesteld dat er na het datalek weliswaar maatregelen zijn getroffen, maar dat de beveiliging op dat moment nog steeds onvoldoende was (**productie K.1**).

104. De AP heeft in het bijzonder onderzocht of voldoende verbetermaatregelen zijn getroffen met het oog op toegangsbeveiliging, verleende autorisaties en autorisatiebeheer, logging van de gebruikte systemen, controle op deze logging en om ongeoorloofd exporteren/printen van persoonsgegevens uit de systemen te voorkomen.

105. De AP heeft met name gewezen op de risico's die verband houden met het grote aantal partijen dat betrokken is bij de verwerking van persoonsgegevens. Volgens de AP zijn er geen duidelijke afspraken tussen de betrokken organisaties. De AP heeft vastgesteld dat dit in het bijzonder geldt ten aanzien van het autorisatiebeheer en de controle van logbestanden. Volgens de AP is als gevolg hiervan onvoldoende duidelijk wie waarvoor verantwoordelijk is en wie welke maatregelen in dit verband dient te treffen. De AP concludeerde dat dit de kans op nieuwe tekortkomingen in de beveiliging van persoonsgegevens vergroot. De AP heeft GGD GHOR en de GGD'en daarom opgedragen om onderling en met de betrokken partijen duidelijke afspraken over informatiebeveiliging te maken, vast te leggen en actueel te houden.

106. Ten aanzien van de vervanging van HPZone (Lite), heeft de AP benadrukt dat reeds bij de ontwikkeling en implementatie van een nieuw systeem de logging en de controle op de logging goed moet worden ingericht zodat regelmatige controle van de logbestanden is verzekerd. Ook benadrukt de AP dat van meet af aan secuur moet worden gekeken naar welke gebruikers welke functionaliteiten nodig hebben en dat autorisaties daarmee in lijn moeten worden gebracht. Ook moet aandacht worden besteed aan de risico's voor de bescherming van persoonsgegevens die gepaard kunnen gaan met een ruime zoekfunctionaliteit.

107. De AP heeft aan GGD GHOR aangegeven geen handhavingstraject op te starten, maar wel gevraagd om een voortgangsrapportage op te leveren. Deze rapportage zou eind februari 2022 aan de AP zijn verstrekt (**productie K.26**).

3.1.10 Datalek groter dan toegegeven

108. RTL Nieuws meldde op 12 augustus 2021 dat de datadiefstal veel meer mensen had getroffen dan het aantal gedupeerden dat GGD GHOR publiekelijk heeft gemeld. RTL onderzocht dit door willekeurig contact op te nemen met een tiental gedupeerden, afkomstig uit één van de datasets die RTL in januari 2021 van criminelen ontving. Deze databestanden bevatten de persoonsgegevens van circa 600 personen, en waren volgens de criminelen die deze datasets aanboden slechts een voorproefje van de gegevens van tienduizenden personen die konden worden geleverd.

109. Geen van de personen waarmee RTL contact opnam bleek een excuusbrief van de GGD te hebben ontvangen of op andere wijze te zijn geïnformeerd. Aldus RTL bestaat hierdoor voldoende aanwijzing dat het aantal gedupeerden van wie gegevens werden gestolen en mogelijk verhandeld, veel hoger ligt dan de 1.250 die een excuusbrief ontvingen. De GGD had maanden na het datalek nog steeds geen goed beeld van hoe groot de datadiefstal echt is, zo schreef RTL (**productie C.17**).

> "De datadiefstal bij de GGD treft veel meer mensen dan het aantal gedupeerden dat de organisatie publiekelijk meldt. […] het daadwerkelijk aantal gedupeerden is echter veel groter, en de GGD heeft na maanden nog geen goed beeld van hoe groot de datadiefstal nu echt is, blijkt uit onderzoek van RTL Nieuws. […] RTL Nieuws heeft willekeurig verschillende mensen opgebeld van wie hun gegevens door criminelen te koop zijn aangeboden. Deze gegevens zijn afkomstig uit twee coronasystemen van de GGD: CoronIT, dat wordt gebruikt voor testen en vaccinaties, en HPZone Lite, het systeem dat wordt gebruikt voor het bron- en contactonderzoek. De personen zijn allemaal niet door de GGD geïnformeerd over dat hun gegevens uit de systemen van de GGD zijn gestolen en mogelijk verhandeld. […] De databestanden, met in totaal de privégegevens van zo'n 600 personen, waren volgens de aanbieders een voorproefje van de vele duizenden tot tienduizenden personen die konden worden geleverd."

110. Naar aanleiding van dit bericht zijn Kamervragen gesteld die op 13 september 2021 door de minister zijn beantwoord (**productie D.11**). In zijn beantwoording gaf de minister aan dat hij contact heeft opgenomen met GGD GHOR. GGD GHOR heeft daarop aangegeven dat uit onderzoek niet is gebleken dat de datadiefstal groter is dan gemeld, of dat er gedupeerden niet zijn geïnformeerd. GGD GHOR geeft aan niet te kunnen vaststellen of de personen die door RTL zijn benaderd daadwerkelijk niet geïnformeerd zijn, omdat RTL de bestanden op journalistieke gronden niet wilde delen en stelde deze inmiddels te hebben verwijderd.

111. Op de vraag hoe het komt dat GGD GHOR onvoldoende in kaart heeft van welke mensen de gegevens zijn gestolen, antwoorde de minister dat GGD GHOR door externe partijen onderzoek heeft laten doen naar de datadiefstal. Uit die onderzoeken zouden geen aanwijzingen naar voren zijn gekomen dat de datadiefstal groter zou zijn dan gemeld. De politie heeft aan GGD GHOR de bestanden die zijn aangetroffen bij verdachten doorgegeven aan GGD GHOR. Op basis van die informatie zijn circa 1.250 mensen door GGD GHOR geïnformeerd.

112. In de FAQ op de website van GGD GHOR schrijft zij over dit onderwerp het volgende (**productie F.15**):

> "Tot op heden, meer dan een jaar na de vermeende datadiefstal, is uit politieonderzoek gebleken dat de gegevens van circa 1.250 personen onbevoegd zijn ingezien, gestolen en mogelijk verkocht. Het gaat om gegevens van personen die bij een GGD een coronatest hebben laten doen of zich bij een GGD hebben laten vaccineren. Deze persoonsgegevens betreffen onder meer naam, adres, telefoonnummer(s), e-mailadres, Burgerservicenummer (BSN), nationaliteit en geboortedatum. De personen van wie deze data zijn gestolen, zijn via een brief door ons geïnformeerd. Voor de vermeende (grootschalige) handel in data uit de coronasystemen is geen bewijs gevonden.

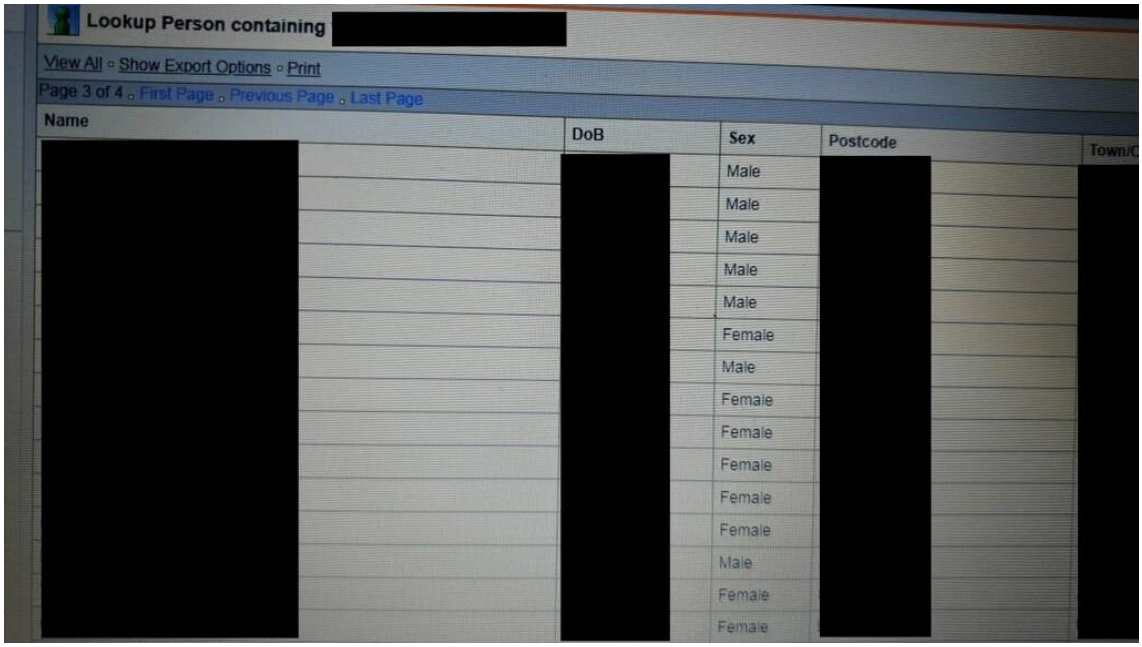
> […]
> Tot nu toe is uit politieonderzoek alleen gebleken dat er uit CoronIT gegevens gestolen zijn. Dit is het administratiesysteem voor het testen en vaccineren en de communicatie hierover. Dus wanneer u een afspraak maakt voor een corona-test via het callcenter, de corona-test website of een arts, komen uw persoonsgegevens in CoronIT. Ook, wanneer u een afspraak maakt voor een vaccinatie.
> […]
> We hebben vernomen dat datasets worden aangeboden, maar hebben nog niet kunnen vaststellen dat ze feitelijk verhandeld zijn. Een jaar na dato heeft de politie dat ook niet vast kunnen stellen. Uit politieonderzoek is alleen gebleken dat de gegevens van circa 1.250 personen onbevoegd zijn ingezien, gestolen en mogelijk verkocht."

113. GGD GHOR geeft dus enkel aan dat zij niet heeft kunnen vaststellen dat grote datasets onbevoegd zijn geëxporteerd uit de GGD-systemen waaronder uit HPZone Lite. Zij blijft echter stil over de vraag of zij kan uitsluiten dat dat gebeurd is (zie ook paragraaf 3.4).

114. Uit een notitie van de GGD Rotterdam-Rijnmond en de daarbij behorende presentatie blijkt dat de GGD er in februari 2021 wel van uitging dat sprake was geweest van "grootschalige downloads van persoonsgegevens" uit HPZone Lite (**productie G.39**). Ook KPMG – dat ook betrokken was bij eerdere risicoanalyses en dat een audit heeft uitgevoerd na het GGD-datalek (paragraaf 1.2.3 en **producties G.56 en G.57**) – meldt in haar privacy-onderzoek van oktober 2021 dat gegevens zijn buitgemaakt uit HPZone Lite en dat gegevens van miljoenen Nederlanders in handen kwamen van kwaadwillenden, die deze via internet doorverkochten (**productie K.2**, p. 6):

> "Zo blijkt 83% op de hoogte van het grote datalek bij de GGD, dat eind januari 2021 bekend werd. Het administratiesysteem voor het test- en vaccinatieproces en de communicatie hierover werd gehackt en ook werden persoonsgegevens rondom het bron- en contactonderzoek van de GGD buitgemaakt. Privégegevens van miljoenen Nederlanders kwamen hierdoor in handen van kwaadwillenden, die de data via internet doorverkochten."

115. Ook reeds uit het eerste onderzoek van RTL in januari 2021 kon dit worden afgeleid (zie ook paragraaf 3.4). Zo blijkt uit screenshots die in dat artikel werden gedeeld dat RTL grote databestanden aangeleverd had gekregen en niet enkel screenshots van CoronIT (**productie C.6**):



3.1.11 Brief van een anonieme ambtenaar

116. Op 23 december 2022 ontving Stichting ICAM een brief van een anonieme ambtenaar, waarschijnlijk bij het ministerie van VWS. In de brief geeft de ambtenaar aan dat het bij het ministerie al in de zomer van 2020 bekend was dat de GGD-systemen "zo lek waren als een mandje". Waarschuwingen hierover werden genegeerd, volgens de ambtenaar mede vanwege persoonlijke belangen van bepaalde personen bij het ministerie (**productie K.23**):

> "De ClO van het ministerie van VWS wist al in de zomer van 2020 dat de systemen van de GGD niet goed beveiligd waren. Dit is hem verteld door de experts die werkten aan de app GGDContact. Dit zijn grotendeels de zelfde mensen die de coronamelder-app hebben gemaakt. De cio van het ministerie van VWS is [redacted], de experts die hem hierop wezen zijn onder andere [redacted], [redacted] en [redacted].
> Op basis van deze informatie is besloten om tussen de app GGDContact en de GGD systemen extra beveiliging in te bouwen. Zo werd gezorgd dat het lek (dat iedereen wist dat zou komen) in de GGD systemen zou komen en niet in de app die het ministerie heeft gemaakt. […]
> Zo'n beetje iedereen die werkte aan de corona-apps wist dit al in de zomer. Over de GGD-systemen sprak iedereen als 'zo lek als een mandje'. De rechterhand van [redacted], mevrouw [redacted], heeft in ieder geval één keer gezegd dat zij vond dat de ClO moest ingrijpen, maar hij wilde dat niet. Zij is kort daarna vertrokken. Vogens de geruchten met ruzie met [redacted]. Mevrouw [redacted] werkt er nog wel en die was er ook bij. Zij moet dit dus ook weten.
> Door niet in te grijpen heeft de cio van VWS toe gestaan dat er persoonsgegevens zijn gelekt. Hij heeft daarna gebruik gemaakt van de problemen bij de GGD om zelf een goede positie te krijgen. Door zijn hulp aan te bieden om te problemen bij de GGD op te lossen heeft hij zijn eigen status vergroot terwijl hij dus al lang wist dat de systemen erg slecht waren beveiligd!
> Het ministerie van VWS liegt dus. hoewel ik niet weet of minister de Jonge weet dat hij liegt."

3.1.12 Financieel gebaar

117. Op 25 april 2022 heeft GGD GHOR de circa 1.250 mensen van wie de politie gegevens heeft gevonden tijdens het onderzoek een brief gestuurd, waarin hen een vergoeding van € 500,- werd aangeboden voor geleden ongemak (**productie F.21**). Indien de gedupeerde het aanbod accepteerde, diende deze – zo blijkt uit de standaardantwoordbrief die moet worden ingevuld - aan GGD GHOR, de GGD'en en andere overheidsinstanties finale kwijting te verlenen:

> "Dit betekent dat u ermee akkoord gaat dat wij tegenover u geen verplichtingen meer hebben die te maken hebben met de datadiefstal uit de coronasystemen van de GGD. Dit geldt dan voor verplichtingen van GGD GHOR Nederland, de GGD'en of andere overheidsinstanties (zoals de gemeente of de landelijke overheid"

118. De Staat c.s. menen dus kennelijk dat het gerechtvaardigd is om Gedupeerden een vergoeding aan te bieden op basis van het enkele feit dat hun persoonsgegevens zijn gestolen. Van enig daadwerkelijk misbruik van de gegevens - in de zin dat de betreffende Gedupeerden daadwerkelijk vermogensschade hebben geleden ten gevolge van bijvoorbeeld *phishing* – is immers ook ten aanzien van deze Gedupeerden niet gebleken.

119. De formulering van de finale kwijting biedt overigens ruimte om ook vorderingen in te stellen namens de Gedupeerden die deze finale kwijting hebben verleend (zie paragraaf 9.1.3.1).

3.2 Getroffen softwaresystemen

3.2.1 CoronIT

120. CoronIT is het administratiesysteem waarin corona test- en vaccinatieafspraken worden gemaakt en waarvandaan uitslagen worden teruggekoppeld aan mensen die getest zijn.[19]

121. De minister heeft GGD GHOR opdracht gegeven "tot gezamenlijke ontwikkeling, implementatie en ondersteuning" van CoronIT, zo blijkt uit de betreffende opdrachtovereenkomst (**productie K.5,** zie ook **productie G.1**, p. 5 e.v.).

122. De minister heeft bij de opdrachtverlening aan GGD GHOR specifieke aanwijzingen en instructies gegeven met betrekking tot de (door)ontwikkeling en inrichting van CoronIT, waaronder met betrekking tot het geautomatiseerd (per-email) bevestigen van afspraken, het delen van uitslagen 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 alle betrokkenen stakeholders. De minister heeft GGD GHOR in dat verband ook opdracht gegeven tot het

[19] *Kamerstukken II* 2020-2021, 27 529, nr. 235, p. 1 (**productie D.3**).

"aansluiten van alle GGD'en op CoronIT". Fase 2 van de opdracht, de doorontwikkeling, omvatte daarnaast ook de ontwikkeling van “data exports en rapportages” (**productie K.5**, artikel 1.2).

123. CoronIT is in opdracht van GGD GHOR vervolgens ontwikkeld en geleverd door IT-bedrijf Topicus.[20] Vanaf mei 2020[21] is CoronIT stapsgewijs in gebruik genomen. De minister heeft alle GGD’en uitdrukkelijk gevraagd CoronIT te implementeren (**productie G.1**, p. 3).

124. Wanneer een afspraak wordt gemaakt voor een coronatest via het callcenter, de corona-testwebsite of een arts, worden persoonsgegevens in CoronIT opgenomen. Dit geldt ook wanneer een afspraak wordt gemaakt voor een vaccinatie (**productie F.15**, p.4). Het proces wordt in de landelijke CoronIT-referentie-DPIA als volgt beschreven (**productie G.1**):

> “Om te zorgen dat het testproces van COVID-19 en de verstrekking van de daaruit volgende uitslag centraal, automatisch, versneld en eenvoudig verloopt, is CoronIT (een webapplicatie) ontwikkeld. In de webapplicatie worden door de aanvrager (bedrijfsarts, instellingsarts, GGD medewerker) of de betrokkene zelf (via een callcenter of portaal) de persoonsgegevens die noodzakelijk zijn voor het testen van de betrokkene ingevuld en wordt vervolgens een afspraak gepland. Aanvullende gegevens worden ingevuld als de betrokkene dit wenst. De gemaakte afspraak wordt automatisch bevestigd aan de betrokkene en voor de afspraak plaatsvindt bevestigd via e-mail en SMS, indien van toepassing ontvangt betrokkene 48 uur voor de afspraak een SMS ter herinnering. De betrokkene wordt getest bij een teststraat van de GGD. Hier worden de door de aanvrager ingevulde gegevens gecontroleerd, waarna bij de betrokkene een monster wordt afgenomen. Het afgenomen monster van de betrokkene wordt door de GGD naar het laboratorium gestuurd. Het betreft hier laboratoria waarmee de GGD (via de Dienst Testen van VWS) afspraken heeft gemaakt inzake het opsturen van monsters. Na ontvangst, worden de monsters door het laboratorium getest en worden de daaruit volgende uitslagen in CoronIT geladen. De aanvrager kan inloggen in de webapplicatie CoronIT om de uitslag te raadplegen. De betrokkene krijgt de uitslag van de test telefonisch via het callcenter of de aanvrager en kan deze inzien via het beveiligde portaal dat is opgezet.”

125. De minister heeft GGD GHOR daarnaast, op grond van een daartoe gesloten dienstverleningsovereenkomst, de opdracht verleend tot "het tot stand brengen en in stand houden van een klantcontactcenter ten behoeve van het maken van afspraken voor het laten uitvoeren van testen ter bestrijding van Covid-19" (**productie K.6**).

126. Volgens GGD GHOR hadden de 25 GGD’en en een aantal landelijke partners toegang tot CoronIT en waren zij gemachtigd accounts aan te maken en gegevens te lezen of toe te voegen.[22] De landelijke partners betroffen op 29 januari 2021 Teleperformance, het Rode Kruis, SOS International, Roamler, Unique en Yacht voor het Landelijk Serviceloket Testen en kort daarvoor ook de Stichting NLOM van VNOW/NCW.

---

20 *Kamerstukken II* 2020-2021, 27 529, nr. 234, p. 14 (**productie D.2**).
21 *Kamerstukken II* 2020-2021, 27 529, nr. 235, p. 7 (**productie D.3**).
22 *Kamerstukken II* 2020-2021, 27 529, nr. 234, p. 30 (**productie D.2**).

127. Medewerkers die betrokken zijn bij testen en vaccineren hebben toegang tot persoonsgegevens in CoronIT (**productie F.15**).[23] Medewerkers van het callcenter die telefoontjes ontvangen kunnen via CoronIT testafspraken en vaccinatieafspraken maken, waarbij onder andere NAW-gegevens, BSN en contactgegevens worden geraadpleegd en vastgelegd. Verder kunnen medewerkers die uitgaande telefoontjes plegen de testuitslagen zien, zodat ze die kunnen meedelen (**productie F.15**). Samen met de medewerkers van gecontracteerde partijen gaat het volgens GGD GHOR om ongeveer 35.000 personen (**productie F.15**). [24]

3.2.2 HPZone (Lite)

128. HPZone is een IT-systeem dat wordt gebruikt voor infectieziektebestrijding van alle typen infectieziekten. Het wordt al sinds 2003 door IT-bedrijf inFact geleverd aan 23 van de 25 GGD'en.

129. Het bron- en contactonderzoek in verband met corona wordt door de GGD'en uitgevoerd in opdracht van het ministerie.[25] Het ministerie heeft GGD GHOR opdracht gegeven uitvoering te geven aan de nationale opschaling van BCO in verband met corona. Meer specifiek: het realiseren van ondersteuning voor het telefonisch BCO, het opleiden van de personen die deze ondersteuning gaan verrichten en het coördineren van deze ondersteuning bij het uitvoeren van BCO. In dit verband is besloten HPZone ook in te zetten voor de bestrijding van corona. Omdat hiervoor een veel groter aantal personen toegang zou krijgen tot het systeem, is in juni 2020[26] HPZone Lite ontwikkeld. De toevoeging "Lite" verwijst naar het feit dat medewerkers die het systeem gebruiken, uitsluitend toegang hebben tot coronadata en niet tot data in verband met andere infectieziektes (**productie F.15**).

130. Gelet op haar opdracht van het ministerie, heeft GGD GHOR het volledige beheer van HPZone overgenomen van de vereniging FBEI. De hosting van HPZone (Lite) is eind 2020 overgegaan. GGD GHOR heeft daartoe een contract met KPN overgenomen en voert daarop ook het accountmanagement uit. GGD GHOR heeft daarnaast het accountmanagement met inFact op zich genomen om de prioritering van de gewenste aanpassingen in HPZone in één hand te beleggen met het oog op de pandemiebestrijding (**productie G.6**). Pas ergens in of na februari 2021 hebben GGD GHOR en de GGD'en, op basis van de opdracht van het ministerie (zie boven en overweging 3 van het convenant), een convenant gegevensuitwisseling gesloten voor de landelijke inzet van BCO en het gebruik van HPZone Lite (**productie G.53**). Wanneer dit convenant exact is getekend en wat de definitieve versie daarvan is, is Stichting ICAM niet bekend.

131. De minister heeft GGD GHOR in dit verband voorts opdracht gegeven "tot het realiseren van digitale randvoorwaarden, waaronder het ontwikkelen en implanteren van digitale ondersteuningsmiddelen voor het bron- en contactonderzoek in de vorm van 'apps'

[23] *Kamerstukken II* 2020-2021, 27 529, nr. 234, p. 70 (**productie D.2**).
[24] *Kamerstukken II* 2020-2021, 27 529, nr. 234, p. 70 (**productie D.2**).
[25] *Kamerstukken II* 2020-2021, 27 529, nr. 234, p. 57 (**productie D.2**).
[26] *Kamerstukken II* 2020-2021, 27 529, nr. 235, p. 1 (**productie D.3**).

(CoronaMelder en Thuisrapportage app), deze in lijn te brengen met de werkprocessen van de GGD en het beheer van het registratiesysteem voor infectieziektebestrijding HPZone landelijk te centraliseren", zo blijkt uit de betreffende opdrachtovereenkomst (**productie K.25**).

132. HPZone Lite was in gebruik bij alle GGD'en en de landelijke schil voor BCO.[27] De 25 GGD'en en de landelijke callcenters die bij BCO betrokken zijn (SOS International, Rode Kruis, Eurocross, ANWB, VHD) hadden toegang tot HPZone Lite en waren gemachtigd om accounts aan te maken en om gegevens te lezen en toe te voegen.[28] Het betreft GGD-artsen en -verpleegkundigen en alle (tijdelijke) medewerkers die bron- en contactonderzoek deden (**productie F.15**). Volgens GGD GHOR ging het in totaal om ongeveer 20.000 medewerkers.[29]

133. Zowel door de minister, GGD GHOR als de GGD'en is erkend dat HPzone niet voldoet aan huidige standaarden (onder andere **producties D.1B**, p. 6**, D.7, C.10 en F.3**). Dit blijkt ook uit externe analyses, waaronder van KPMG en IT-bedrijf Axis (**producties G.55 t/m G.58**). De minister van VWS, GGD GHOR en de GGD'en hebben samen gewerkt aan het vervangen van HPZone Lite. De minister heeft GGD GHOR in dat verband gevraagd de vervanging van HPZone landelijk te coördineren en aangegeven hierbij op verzoek van GGD GHOR als opdrachtgever te zullen optreden.[30] Het nieuwe systeem, GGD Contact, wordt onder verantwoordelijkheid van de minister gebouwd en daarna door de GGD'en geïmplementeerd.[31]

3.3 Persoonsgegevens in de getroffen systemen

3.3.1 CoronIT

134. CoronIT bevat volgens GGD GHOR onder meer naam, adres, woonplaats, telefoonnummer, e-mailadres, BSN, geslacht, geboortedatum, test- en/of vaccinatieafspraken, testresultaten, contra-indicaties en corona klachten (**productie F.15**).[32]

135. Volgens de privacyverklaring 'testen op het coronavirus' van GGD GHOR, worden de volgende persoonsgegevens verzameld en gedeeld met de IT-provider van CoronIT (Topicus) (**productie F.16**):

- Voornaam & achternaam
- Adres, of een andere plaats waar u bent als u niet thuis bent. Bijvoorbeeld op vakantie.
- Geboortedatum
- Of u man of vrouw bent, niet gespecificeerd of onbekend

---

27 *Kamerstukken II* 2020/21, 27 529, nr. 234, p. 17 (**productie D.2**).
28 *Kamerstukken II* 2020/21, 27 529, nr. 234, p. 30 (**productie D.2**).
29 *Kamerstukken II* 2020/21, 27 529, nr. 234, o.a. p. 3 (**productie D.2**).
30 *Kamerstukken II* 2020-2021, 27 529, nr. 235, p. 2 (**productie D.3**), zie ook **productie K.1.**
31 *Kamerstukken II* 2020/21, 25 295, nr. 1179, p. 41 (**productie D.9**); *Kamerstukken II* 2020-2021, 25 295, nr. 1105, p. 35 (**productie D.8**).
32 *Kamerstukken II* 2020-2021, 27 529, nr. 234, p. 21 (**productie D.2**).

- Burger Service Nummer (BSN)
- Telefoonnummer
- E-mailadres
- Uw klachten
- Streepjescode testbuisje
- Uitslag van de coronatest
- Eventueel: naam van de arts die de test aanvraagt
- Of u direct contact heeft gehad met anderen
- Of u gewerkt heeft, en zo ja, in welke beroepsgroep u werkt

136. Voor het uitvoeren van vaccinaties worden volgens de privacyverklaring 'vaccinatie tegen het coronavirus' van GGD GHOR de volgende persoonsgegevens verwerkt in CoronIT (**productie F.17**):

- Voornaam & achternaam
- Of u man of vrouw bent, niet gespecificeerd of onbekend
- Burger Service Nummer (BSN)
- Telefoonnummer
- E-mailadres
- Doelgroep waarbij u hoort
- Medische gegevens, om te bepalen of u een vaccinatie kunt krijgen (contra-indicaties en medische triage)
- Gegevens over het vaccin dat u krijgt: vaccinnaam en – nummer
- Naam van uw arts

137. Volgens de CoronIT-referentie-DPIA worden de volgende gegevens in het systeem verwerkt (**productie G.1**):

Persoonsgegeven	Gewoon persoonsgegeven	Bijzonder persoonsgegeven	Wettelijk identificerend persoonsgegeven
Voornaam en achternaam	Ja		
Geboortenaam partner (optioneel)	Ja		
Voorletters/roepnaam (optioneel)	Ja		
Postcode	Ja		
Huisnummer	Ja		
Straatnaam	Ja		
Woonplaats	Ja		
Gemeente	Ja		
Land	Ja		
Gekoppelde GGD	Ja		
Telefoonnummer (optioneel)	Ja		
E-mail	Ja		
Geslacht	Ja		
BSN			Ja
Barcode buisje	Ja		
Patiëntnummer	Ja		
Of de persoon de laatste 2 weken heeft gewerkt en zo ja, waar	Ja		
Checklist klachten		Ja	
Aantal afspraken bij GGD locaties		Ja	
Testuitslag		Ja	

3.3.2 HPZone Lite

138. Volgens GGD GHOR stonden in HPZone Lite onder meer naam, adres, woonplaats, telefoonnummer, geslacht, geboortedatum en BSN van een persoon. Verder wordt in HPZone Lite ook de informatie uit de bron- en contactonderzoeksgesprekken vastgelegd. Dit zijn onder andere gegevens over corona-gerelateerde 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 (**productie F.15**).[33]

139. Een uitgebreide weergave van de persoonsgegevens zoals geregistreerd in HPZone Lite is te vinden in de 'privacyverklaring landelijke capaciteit bron- en contactonderzoek COVID-19' (**productie F.18**):

POSITIEF GETEST PERSOON

[33] *Kamerstukken II* 2020-2021, 27 529, nr. 234, p. 21 (**productie D.2**).

- Voornaam en achternaam
- Geboortedatum
- BSN
- Moedertaal positief getest persoon
- Telefoonnummer
- E-mailadres
- Gegevens over uw huisarts
- De datum van uw (positieve) coronatest en de reden van testen
- Gegevens over uw klachten (waaronder de begindatum, soort en het verloop)
- Datum start besmettelijke periode
- Behoren tot medische risicogroep
- Sprake van gestoorde afweer
- Gegevens over uw (eventuele) ziekenhuisopname
- Eventueel overlijden en doodsoorzaak (COVID-19 of anders)
- Huidige verblijfplaats (e.g. zorginstelling, asielzoekerscentrum, serviceflat, studentenhuis) i.v.m. isolatiemogelijkheden
- Gegevens over uw beroep (waaronder sector, laatste werkdag, informeren

werkgever en collega's)

- Gegevens over uw (eventuele) thuiszorg of mantelzorger en diens contactgegevens
- Gegevens over de settingen waarin u bent geweest tijdens uw besmettelijke periode
- (zoals zorginstelling, sport, onderwijs)
- Toestemming om naam te noemen aan contacten, werk/instelling, en huisarts

BRONONDERZOEK

- Gegevens over een (eventueel) bezoek aan het buitenland (waaronder data, land en vervoersmiddel)
- Of er mensen in uw omgeving zijn met klachten passend bij COVID-19
- Gegevens over of u contact hebt gehad met een bewezen coronapatiënt

Indien van toepassing:

- Volledige naam (geboorte- en partnernaam) bewezen coronapatiënt
- Geboortedatum bewezen coronapatiënt
- (Eventueel) bekende dossiernummers van bewezen coronapatiënt

CONTACTONDERZOEK

- Van huisgenoten
    - Voornaam en achternaam
    - Geboortedatum
    - BSN
    - Relatie tot positief getest persoon
    - Telefoonnummer
    - E-mailadres
    - Laatste contactmoment
    - Mogelijkheid isolatie
    - Minimale datum einde quarantaine voor huisgenoten/gezin
    - Datum PCR-test

- Van nauwe contacten
    - Voor- en achternaam
    - Geboortedatum
    - BSN
    - Telefoonnummer
    - E-mailadres
    - Datum & aard laatste contact
    - Datum einde quarantaine voor contact
    - Datum PCR-test
    - Beroep

3.4 Omvang

140. Het GGD-datalek is van ongekende omvang. Ten tijde van de berichtgeving door RTL Nieuws in januari 2021 stonden volgens GGD GHOR persoonsgegevens van circa 5,5 miljoen personen in CoronIT en van circa 1 miljoen personen in HPZone (**productie F.15**). Van al deze personen zijn zeer gevoelige, risicovolle en deels bijzondere persoonsgegevens gecompromitteerd geweest. Al deze 6,5 miljoen mensen leven in onzekerheid of hun gegevens zijn gestolen en mogelijk zelfs zijn verhandeld in het criminele circuit. Zeer waarschijnlijk worden grote databestanden met gegevens uit het GGD-datalek aangeboden op het *darkweb* en niemand weet zeker of zijn of haar gegevens daarin zijn opgenomen.

141. Na afronding van het politieonderzoek berichtte GGD GHOR dat is vastgesteld dat de gegevens van circa 1.250 personen uit CoronIT zijn gestolen en mogelijk verkocht. GGD GHOR schreef op 5 april 2022 op haar website: "*Eind januari 2021 werden de GGD'en opgeschrikt doordat RTL het bericht naar buiten bracht dat grote databestanden uit de coronasystemen in omloop zouden zijn. De politie heeft hier echter geen aanwijzingen voor gevonden. De politie heeft wel kunnen vaststellen dat door de verdachten screenshots zijn gemaakt met daarop persoonsgegevens van zo'n 1250 personen*."(**productie F.19**).

142. Uit deze bewoordingen volgt dat de Staat c.s. kennelijk niet sluitend kunnen vaststellen van hoeveel personen daadwerkelijk gegevens zijn ontvreemd en/of verkocht.

143. Ten eerste verklaart GGD GHOR slechts dat de politie "geen aanwijzingen" heeft gevonden dat grote databestanden in omloop zijn. De politie heeft kennelijk echter ook niet vast kunnen stellen dat *geen* grote databestanden in omloop zijn. Dat daarvoor geen aanwijzingen zijn gevonden, sluit de mogelijkheid echter niet uit. Als die mogelijkheid wel zou kunnen worden uitgesloten, of als de kans daarop heel klein zou zijn, dan zou te verwachten zijn dat GGD GHOR hierover explicieter zou zijn.

144. GGD GHOR heeft in het overleg met Stichting ICAM aangegeven dat zij naar aanleiding van het GGD-datalek forensisch onderzoek heeft laten doen en het forensisch rapport aan de politie heeft verstrekt. Zij weigert het rapport echter te verstrekken aan Stichting ICAM en onduidelijk

is of de politie het forensisch onderzoek heeft betrokken in haar eigen onderzoek. Ook heeft GGD GHOR in het overleg met Stichting ICAM geen antwoord willen geven op de vraag of er logfiles zijn van het gebruik van de exportmogelijkheid in HPZone Lite (hetgeen waarschijnlijk de bron is van de grote databestanden waarover RTL Nieuws heeft bericht (paragraaf 3.1.3)) of op de vraag of er in het forensisch onderzoek en/of in het politieonderzoek logfiles zijn onderzocht. Hoogstwaarschijnlijk willen de Staat c.s. hierover geen openheid van zaken geven omdat uit het forensisch rapport blijkt dat er niet goed is gelogd en/of dat er geen logfiles (beschikbaar) zijn. Als die logfiles er wel zouden zijn, en als die zouden zijn onderzocht naar aanleiding van het GGD-datalek, dan zou GGD GHOR met meer zekerheid moeten kunnen vaststellen dat geen grote databestanden zijn geëxporteerd uit HPZone Lite. Uit het feit dat er gebrekkig of helemaal niet is gelogd, kan uiteraard niet de conclusie worden getrokken dat er geen grote databestanden zijn gestolen. De Staat c.s. kunnen dit simpelweg niet vaststellen.

145. Ten tweede is de vaststelling dat gegevens van 1.250 personen zijn gestolen en mogelijk verkocht, kennelijk uitsluitend gebaseerd op screenshots die door de verdachten zijn gemaakt. Het lijkt er sterk op dat de politie haar conclusies heeft gebaseerd op bij de verdachten inbeslaggenomen gegevensdragers waarop de screenshots zijn aangetroffen (**producties J.1 t/m J.5**). RTL Nieuws berichtte echter dat er tientallen accounts waren op onder andere Telegram en Wickr: ''andere accounts bieden grote datasets aan met daarin de privégegevens van vele tienduizenden Nederlanders. Criminelen vragen hier duizenden euro's voor omdat het relatief uniek is dat er op zo'n grote schaal Burgerservicenummers worden verkocht. Een Burgerservicenummer is zeer gevoelig en kan worden misbruikt voor identiteitsfraude.'' (**productie C.6 en C.14**). Onduidelijk is of al deze accounts werden beheerd door de acht verdachten die de politie heeft aangehouden. Het is goed mogelijk dat de politie niet alle daders in beeld heeft kunnen brengen en er dus mogelijk meer gegevens zijn ontvreemd en/of verkocht.

146. De omstandigheid dat RTL Nieuws wel grote databestanden heeft aangetroffen en verkregen (paragraaf 3.1.3) wijst er op dat er wel degelijk misbruik is gemaakt van de exportmogelijkheid in HPZone Lite.

147. Stichting ICAM heeft aanwijzingen dat op het *darkweb* daadwerkelijk grote databestanden uit het GGD-Datalek voorhanden zijn. Zij heeft dat momenteel nog in onderzoek.

148. Naar overtuiging van Stichting ICAM c.s. is de groep van personen van wie gegevens zijn ontvreemd en/of verkocht dus vele malen groter dan de Staat c.s. stellen. De daadwerkelijke omvang van deze groep personen heeft zij tot op heden echter niet kunnen vaststellen.

3.5 Duur

149. Het GGD-datalek is niet alleen qua omvang ongekend, maar ook qua duur. De grootste risico's hebben maar liefst elf maanden bestaan. Voor zover op dit moment bekend, is de beveiliging

echter ook op de datum van dagvaarding – bijna drie na ingebruikname van de GGD-systemen - nog altijd niet op een adequaat niveau.

150. Het GGD-datalek is door RTL Nieuws op 25 januari 2021 in volle omvang bekendgemaakt (paragraaf 3.1.3). Toen bleek dat de beveiliging van de GGD-systemen al sinds de ingebruikname daarvan tekortschoot. HPZone is vanaf maart 2020 ingezet voor BCO bij coronabesmettingen. CoronIT is begin juni 2020 in gebruik genomen.

151. In de periode nadat het GGD-datalek bekend werd hebben de Staat c.s. een aantal maatregelen genomen. Onder andere zijn de printfunctionaliteit in CoronIT en de exportfunctionaliteit in HPZone Lite op 25 januari 2021 uitgezet. De exportfunctionaliteit in HPZone Lite is daarna weer beschikbaar gemaakt voor een beperkt aantal medewerkers. De printfunctionaliteit in HPZone Lite is op 30 januari 2021 uitgezet. Ook zijn na de RTL Nieuws-berichtgeving de toegang en zoekfunctionaliteiten van de GGD-systemen aangepast, hoewel onduidelijk is wat daaraan exact is gewijzigd. Ten slotte zijn de Staat c.s. na de berichtgeving begonnen met het dagelijks controleren op verdachte activiteiten.

152. Door deze eerste maatregelen is het risico op verdere ongeautoriseerde toegang tot persoonsgegevens en het risico op verdere ongeautoriseerde onttrekking van gegevens aan de systemen, waarschijnlijk kleiner geworden. In de periode voordat de maatregelen werden getroffen, waren die risico's echter zeer groot, en hebben die risico's zich ook verwezenlijkt.

153. Echter, ook nadat de Staat c.s. eind januari/begin februari 2021 maatregelen hebben genomen, was de beveiliging van de GGD-systemen nog altijd niet op orde, zo concludeerde de AP in november 2021 (paragraaf 3.1.9). Of de GGD-systemen momenteel wel voldoen aan alle wettelijke vereisten, is Stichting ICAM niet bekend. De Staat c.s. hebben de voortgangsrapportage die zij aan de AP hebben verstrekt (paragraaf 3.1.9 en **productie 26**), niet openbaargemaakt of aan Stichting ICAM verstrekt. Stichting ICAM kan dus niet vaststellen of de beveiliging sindsdien voldoende is.

3.6 Conclusie: beveiligingsgebreken

154. Samenvattend volgt uit het voorgaande dat de GGD-systemen de volgende feitelijke beveiligingsgebreken kennen althans kenden:

a) Medewerkers konden via eigen apparatuur en buiten een beveiligde omgeving inloggen op de GGD-systemen;

b) Ongeveer 35.000 (deels extern ingehuurde) GGD-medewerkers hadden in CoronIT toegang tot veel meer gevoelige en bijzondere persoonsgegevens dan waar zij toegang tot nodig hadden voor hun werkzaamheden, van in totaal ten minste 5,5 miljoen mensen;

c) Ongeveer 20.000 (deels extern ingehuurde) GGD-medewerkers hadden in HPZone Lite toegang tot veel meer gevoelige en bijzondere persoonsgegevens dan waar zij toegang tot nodig hadden voor hun werkzaamheden, van in totaal ten minste 1 miljoen mensen;

d) HPZone Lite bevatte een niet-noodzakelijke exportfunctionaliteit waarmee grote datasets konden worden gedownload. Deze functionaliteit was ten onrechte beschikbaar voor alle (deels extern ingehuurde) GGD-medewerkers;

e) CoronIT bevatte een niet-noodzakelijke printfunctionaliteit, met als gevolg dat grote datasets geprint konden worden. Deze functie was niet alleen onnodig voor de uitvoering van de opgelegde taak, maar tevens kon een onnodig grote groep medewerkers hiervan gebruik maken. Dit samen heeft geleid tot een situatie waarin het niet alleen lastig is om de (geprinte) data controleerbaar te houden, maar ook om eenmaal geprinte gegevens veilig te stellen (en te houden);

f) Beide GGD-systemen bevatten zoekfunctionaliteiten waarmee veel specifieker en veel breder persoonsgegevens konden worden opgezocht dan noodzakelijk was;

g) Niet alle relevante gebruikershandelingen werden (afdoende) gelogd en logbestanden werden niet systematisch en consistent gecontroleerd;

h) Verplichte NEN-normen werden niet toegepast;

i) Persoonsgegevens waren niet gepseudonimiseerd;

j) Gebruikers konden toegang krijgen tot systemen zonder de vereiste verklaring van goed gedrag te overleggen;

k) Gebruikers waren niet voldoende getraind en geïnstrueerd; en

l) Gebruikers hadden na beëindiging van hun dienstverband nog toegang tot systemen.

155. De gebreken zullen verder worden uitgewerkt in hoofdstuk 4. Dat de beveiliging niet voldeed aan de AVG is reeds geconstateerd door de AP en erkend door de minister en GGD GHOR (mede namens de GGD'en), maar volgt, zoals hierna zal blijken, ook uit de Woo-stukken.

4 SCHENDINGEN VAN HET RECHT

156. In dit hoofdstuk zal Stichting ICAM uiteenzetten op welke wijze de Staat c.s. het recht hebben geschonden. In paragraaf 4.1 behandelt zij de schending van fundamentele (verdrags)rechten, in paragraaf 4.2 de (omvangrijke) AVG-schendingen en in paragraaf 4.3 de schending van enkele zorgspecifieke wettelijke bepalingen.

4.1 Schending van fundamentele rechten

157. Met meer dan 6,5 miljoen Gedupeerden is het GGD-datalek het grootste datalek in de Nederlandse geschiedenis. Van deze Gedupeerden zijn niet alleen gewone persoonsgegevens opgeslagen in de systemen, maar ook bijzondere (medische) persoonsgegevens. Juist met bijzondere persoonsgegevens dient extra zorgvuldig te worden omgegaan.

158. De Staat c.s. hebben hun taak veronachtzaamd om (bijzondere) persoonsgegevens, opgeslagen in de systemen van publieke instellingen, adequaat te beveiligen. Door na te laten adequate (beveiligings)maatregelen te treffen, hebben de Staat c.s. een risico op een grootschalig datalek doen ontstaan, welk risico zich vervolgens ook heeft verwezenlijkt. Bovendien hebben de Staat c.s. onvoldoende inspanningen geleverd om de omvang van het datalek vast te stellen. Deze handelswijze van de Staat c.s. vormt niet alleen een inbreuk op de AVG, maar ook een ernstige inmenging in de fundamentele rechten van de Gedupeerden. In het bijzonder maakt zij inbreuk op het recht op eerbiediging van het privéleven, neergelegd in respectievelijk artikel 8 EVRM en artikel 7 Handvest, en het recht op gegevensbescherming, neergelegd in artikel 8 Handvest.

159. Het recht op privacy en gegevensbescherming is een grondrecht, zo bevestigt overweging 1 van de AVG onder verwijzing naar artikel 8 Handvest. Deze grondrechtelijke context moet worden meegenomen in de beoordeling van de onderhavige zaak.

160. Het Handvest is gericht op lidstaten wanneer zij Unierecht, zoals de AVG, ten uitvoer leggen.[34] Voor zover het Handvest rechten bevat die corresponderen met rechten die door het EVRM gegarandeerd worden, zoals het recht op eerbiediging van het privéleven, is de inhoud en reikwijdte daarvan op grond van artikel 52 lid 3 Handvest hetzelfde. Artikel 7 en 8 Handvest zijn bovendien gebaseerd op artikel 8 van het EVRM en moeten om die reden eenduidig geïnterpreteerd worden.[35]

161. Het recht op eerbiediging van het privéleven uit artikel 8 EVRM kent een ruime uitleg en omvat ook het recht op gegevensbescherming.[36] Artikel 8 Handvest bevat ook een zelfstandig recht op gegevensbescherming. Eerbiediging van dat recht hangt sterk samen met het recht op eerbiediging van het privéleven uit artikel 7 Handvest, zo bevestigt het HvJEU.[37] Immers, een inbreuk op het recht op gegevensbescherming kan ook (significante) gevolgen met zich meebrengen voor het privéleven. Dat is in het bijzonder het geval als het gezondheidsgegevens betreft. Het EHRM heeft met betrekking tot deze categorie van persoonsgegevens expliciet geoordeeld dat zij een essentieel onderdeel vormt van het privéleven.[38] Bovendien is het

[34] Artikel 51 lid 1 Handvest.
[35] S. Peers e.a., *The EU Charter of Fundamental Rights: A Commentary*, Oxford: Hart Publishing 2014, p. 155.
[36] EHRM 8 december 2008, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper/Verenigd Koninkrijk*), r.o. 41.
[37] HvJEU 8 april 2014, ECLI:EU:C:2014:238, (*Digital Rights Ireland*), r.o. 53.
[38] Zie onder meer: EHRM 10 oktober 2006, ECLI:CE:ECHR:2006:1010JUD000750802 (*L.L./Frankrijk)*, r.o. 44.

respecteren van de vertrouwelijkheid van deze gegevens cruciaal omdat burgers moeten kunnen vertrouwen op gezondheidsdiensten.[39]

162. Op lidstaten rust een positieve verplichting om de effectieve uitoefening van het recht op privéleven en het recht op gegevensbescherming te garanderen.[40] Dat houdt in dat lidstaten actief maatregelen moeten nemen om voornoemde verdragsrechten te waarborgen. Doordat de Staat c.s. hebben nagelaten adequate maatregelen te treffen om het GGD-datalek te voorkomen, heeft zij de fundamentele rechten van de Gedupeerden en haar positieve verplichting om de effectieve uitoefening van die rechten te garanderen geschonden.

4.2 Inbreuken op de AVG

163. Om de veiligheid van Betrokkenen te waarborgen en te voorkomen dat een verwerking van persoonsgegevens inbreuk maakt op de AVG, dient een verwerkingsverantwoordelijke de aan de verwerking inherente risico's te beoordelen en maatregelen te treffen om deze risico's te beperken. Die maatregelen dienen een passend niveau van beveiliging te waarborgen, rekening houdend met de stand van de techniek en de uitvoeringskosten, afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens. Gezondheidsgegevens behoren vanwege de gevoeligheid ervan tot een bijzondere categorie van persoonsgegevens. Om deze reden gelden voor de bescherming van die gegevens zeer hoge eisen.

164. Met passende beveiligingsmaatregelen wordt bijgedragen aan het behoud van vertrouwen van Betrokkenen in de Staat c.s. bij de omgang met persoonsgegevens. Om te bepalen of beveiligingsmaatregelen passend zijn, wordt, onder andere door de AP, aangesloten bij algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging. In dit geval is dat de praktijk in de zorg.

165. Dat de AVG zowel materieel, territoriaal als temporeel van toepassing is op deze zaak staat niet ter discussie.

4.2.1 Verwerkingsverantwoordelijken

166. 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

[39] Zie onder meer: EHRM 25 februari 1997, ECLI:CE:ECHR:1997:0225JUD002200993 (*Z/Finland)*, r.o. 95.
[40] EHRM 13 juni 1979, ECLI:CE:ECHR:1979:0613JUD000683374 (*Marckx/België*), r.o. 31.

in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen."

167. Een verwerkingsverantwoordelijke is een orgaan dat beslist over bepaalde belangrijke elementen van de verwerking. Deze verantwoordelijkheid kan bij wet worden vastgesteld of kan voortvloeien uit een analyse van de feitelijke elementen of omstandigheden van het geval. In dat verband dienen de volgende vragen in overweging te worden genomen:[41]

a) Waarom vindt deze verwerking plaats? Dat wil zeggen "met welk doel" of "waarvoor";

b) Wie heeft besloten dat de verwerking voor een bepaald doel moet plaatsvinden en hoe vindt de verwerking plaats? Welke middelen worden ingezet om het doel te bereiken?.

168. Volgens de EDPB kunnen in veel gevallen de contractuele afspraken tussen de verschillende betrokken partijen een aanwijzing zijn om vast te stellen welke partij als verwerkingsverantwoordelijke optreedt. Zelfs indien in een overeenkomst niet wordt vermeld wie de verwerkingsverantwoordelijke is, kan deze voldoende elementen bevatten om uit te maken wie een besluitvormende rol vervult met betrekking tot het doel en de middelen van de verwerking.[42]

169. Wat de vaststelling van de middelen betreft, kan een onderscheid worden gemaakt tussen wezenlijke en niet-wezenlijke middelen. "Wezenlijke middelen" worden gewoonlijk voorbehouden aan de verwerkingsverantwoordelijke. "Wezenlijke middelen" zijn middelen die nauw verband houden met het doel en de reikwijdte van de verwerking, zoals het soort persoonsgegevens dat wordt verwerkt ("welke gegevens worden verwerkt?"), de duur van de verwerking ("hoelang worden zij verwerkt?"), de categorieën ontvangers ("wie heeft daartoe toegang?") en de categorieën betrokkenen ("van wie worden persoonsgegevens worden verwerkt?").[43]

170. Wie het doel van de verwerking vaststelt, wordt tegen deze achtergrond dan in ieder geval als voor de verwerking verantwoordelijk aangemerkt, terwijl bij het vaststellen van de middelen alleen van verantwoordelijkheid sprake is wanneer die vaststelling betrekking heeft op de wezenlijke aspecten van de middelen.

171. De kwalificatie "gezamenlijke verwerkingsverantwoordelijken" doet zich voor wanneer met betrekking tot een specifieke verwerkingsactiviteit verschillende partijen gezamenlijk het doel en de middelen van deze verwerkingsactiviteit bepalen. Het feit dat één van de partijen geen

41 EDPB, 'Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG', Vastgesteld op 7 juli 2021, p. 12.
42 EDPB, 'Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG', Vastgesteld op 7 juli 2021, p. 15.
43 EDPB, 'Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG', Vastgesteld op 7 juli 2021, p. 17.

toegang heeft tot verwerkte persoonsgegevens, volstaat volgens de EDPB niet om de gezamenlijke verantwoordelijkheid voor de verwerking uit te sluiten.[44]

172. Iedere verwerkingsverantwoordelijke dient er onder andere voor in te staan dat persoonsgegevens worden verwerkt op een wijze die rechtmatig, behoorlijk en transparant is (artikel 5 lid 1 onderdeel a AVG), dat de persoonsgegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (artikel 5 lid 1 onderdeel c AVG) en dat de integriteit en vertrouwelijkheid gewaarborgd blijven (artikel 5 lid 1 onderdeel f AVG). De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van deze beginselen en moet ook kunnen aantonen dat een verwerking van persoonsgegevens aan deze beginselen voldoet (de verantwoordingsplicht). Concreet dient de verwerkingsverantwoordelijke hiertoe onder meer voorafgaand aan risicovolle verwerkingsactiviteiten een gegevensbeschermingseffectbeoordeling uit te voeren (artikel 35 AVG), bij het inrichten van verwerkingen rekening te houden met de principes van privacy door ontwerp en door standaardinstellingen (*privacy by design* en *privacy by default*; artikel 25 AVG) en passende beveiligingsmaatregelen te treffen met het oog op de bescherming van persoonsgegevens (artikel 32 AVG).

4.2.1.1 Primair: De Staat (ministerie van VWS)

173. Stichting ICAM stelt zich primair op het standpunt dat de Staat (het ministerie van VWS) is aan te merken als zelfstandig verwerkingsverantwoordelijke.

174. Ten eerste heeft de Staat het doel van de gegevensverwerkingen door de GGD'en bepaald. De minister heeft op grond van artikel 3 Wpg de taak om de kwaliteit en doelmatigheid van de publieke gezondheidszorg te bevorderen en zorg te dragen voor de instandhouding en verbetering van de landelijke ondersteuningsstructuur.

175. Het testen op corona en het uitvoeren van BCO bij corona is geen wettelijke taak van de GGD'en. De besturen van de veiligheidsregio's zijn, ingevolge artikel 6 lid 2 Wpg, in geval van een epidemie behorend tot groep A, zoals corona, verantwoordelijk voor de voorbereiding van de bestrijding hiervan. De voorzitters van de veiligheidsregio's zijn, ingevolge artikel 6 lid 4 Wpg, verantwoordelijk voor de bestrijding van een dergelijke epidemie. De leiding ligt, ingevolge artikel 7 lid 1 Wpg, echter bij de minister, die in dat verband de voorzitters van de veiligheidsregio's kan opdragen hoe de bestrijding ter hand te nemen.

176. De Staat heeft bij de uitbraak van de corona-pandemie in Nederland aan de GGD'en gevraagd om in aanvulling op hun wettelijke taken inzake de infectieziektebestrijding, het testen en

[44] C-210/16, ECLI:EU:C:2018:388 (*Wirtschaftsakademie*), punt 38

traceren van mensen met klachten die passen bij corona uit te voeren. Dit ondanks het feit dat zij niet voorbereid waren op een taak van deze omvang:

> "Bij de uitbraak van de covid-19 pandemie in Nederland, heb ik de GGD'en gevraagd om aanvullend op, maar passend bij hun reguliere, wettelijke taken inzake de infectieziektebestrijding, het testen (en traceren) van mensen met klachten die passen bij covid-19 uit te voeren. Het testen op covid-19 is geen wettelijke taak van de GGD'en, maar is wel een taak die logischerwijs bij de GGD'en belegd is. Het afnemen van diagnostiek is bijvoorbeeld wel een standaard onderdeel van het generieke draaiboek voor grootschalige infectieziektebestrijding van de Landelijke Coördinatie Infectieziektebestrijding (LCI). De GGD'en zijn daarom de meest aangewezen organisaties om deze noodzakelijke taak uit te voeren, ondanks dat zij niet voorbereid waren op een taak van deze omvang."[45]

177. Ten tweede heeft de Staat wezenlijke aspecten van de middelen voor gegevensverwerking vastgesteld:

a) De Staat heeft in april/mei 2020 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 (**productie K.5**). Voorts heeft de Staat GGD GHOR opdracht gegeven een klantcontactcentrum op te richten om testafspraken te kunnen inplannen (**productie K.6**);

b) Uit de gang van zaken rondom de ontwikkeling van een vervanging voor HPZone (Lite) blijkt dat de Staat ook bij de keuze voor dat systeem een beslissende rol heeft vervuld. Ook uit het feit dat de Staat naar aanleiding van het GGD-datalek opdracht heeft gegeven om HPZone te vervangen, blijkt dat hij beslissende zeggenschap had over de inzet van HPZone voor BCO ten behoeve van de bestrijding van de coronapandemie.[47] Voorgaande blijkt ook uit de DPIA die is opgesteld ten behoeve van de ontwikkeling van GGD Contact (**productie G.33**, zie o.a. p. 18), de applicatie die HPZone gaat vervangen:

> "• Sinds maart 2020 heeft Nederland te maken met de infectieziekte COVID-19. Gelet op de grootschaligheid van deze infectieziekte en de noodzaak van het snel en efficiënt handelen ter voorkoming of beperking van de verspreiding ervan is door de 'Begeleidingscommissie Digitale Ondersteuning Bestrijding Covid-19' van VWS gekeken naar digitale verbetermogelijkheden die

[45] *Kamerstukken II* 2020-2021, 27 529, nr. 235 (**productie D.3**).
[46] Feitenrelaas inzake gebeurtenissen omtrent coronatest-IT-systeem van de GGD, bijlage bij *Kamerstukken II* 2020-2021, 27 529, nr. 236 (**productie D.6**).
[47] Zie ook: Ministerie van Volksgezondheid, Welzijn en Sport, 'Kamerbrief over stand van zaken digitale ondersteuning pandemiebestrijding,' 12 februari 2021, p.1 (**productie D.7**).

ondersteunend hiervoor kunnen zijn. Medio april 2020 heeft VWS ten aanzien van de digitale mogelijkheden ter bestrijding van COVID-19 een marktconsultatie gedaan. Vanuit de wens van GGD'en heeft de brancheorganisatie GGD GHOR Nederland VWS gevraagd om ondersteuning te bieden in de realisatie van GGD Contact, waarbij de minister een wettelijke verantwoordelijkheid heeft met betrekking tot het bestrijden van infectieziektebestrijding [sic.]. De realisatie van GGD Contact (release 1.0) heeft plaatsgevonden binnen het VWS-programma Realisatie Digitale Ondersteuning (RDO).
• In opdracht van de minister van VWS dient HPZone vervangen te worden.[4] Op 12 februari 2021 heeft de DPG-raad besloten om HPZone Lite te vervangen op korte termijn. Het gekozen scenario voor de vervanging op korte termijn en de functionaliteiten die deze bevat wordt aangemerkt als release 1.1. De keuze en afweging voor GGD Contact is nader in de daarvoor uitgewerkte beslisnotities uitgewerkt."

c) De Staat had beslissende zeggenschap over het aannemen van medewerkers voor testen, vaccineren en BCO (**productie G.29**);

d) Voor zowel CoronIT als HPZone (Lite) geldt dat de Staat "uiteindelijk bepaalde" of functies werden aan-of uitgezet, waaronder de exportfunctie in HPZone (Lite) (**productie G.28**);

e) GGD GHOR-voorzitter André Rouvoet heeft bevestigd dat "het de rol is van VWS om een balans te zoeken tussen de virusbestrijding enerzijds, en de eisen die je stelt aan o.a. beveiliging anderzijds. Die beleidskeuze liggen bij de minister." (**productie G.28**);

f) GGD GHOR-voorzitter André Rouvoet heeft – in de context van een update over de stand van zaken rondom het GGD-datalek - aangegeven dat er "voor A-ziekten oekazes komen van de minister, die verantwoordelijk is." (**productie G.28**);

g) De Staat acht zichzelf ook verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens in de corona notificatieapp, die bedoeld is om de GGD'en te ondersteunen bij BCO (**productie G.31, overweging (d)**);

h) Het ministerie had een "centrale regierol die voortvloeit uit de toepassing van art. 6 en 7 Wpg". (**productie G.32**);

i) In een e-mailwisseling van de gemeente Rotterdam wordt vermeld dat "de minister de prioriteiten bepaalt (eerst bv. Beveiligen of eerst de registratie op orde)." (**productie G.34**);

j) In een advies van Dirkzwager aan de GGD Noord- en Oost-Gelderland, adviseert Dirkzwager weliswaar niet over de vraag of de Staat mogelijk als verwerkingsverantwoordelijke moet worden aangemerkt, maar signaleert het advocatenkantoor wel enkele aanknopingspunten die tot die conclusie leiden: "Eind mei heeft VWS besloten dat er [sic.] de GGD'en zouden gaan werken met een landelijke pool van zogeheten BCO-medewerkers en daarnaast tot onderlinge personele ondersteuning

tussen GGD'en. HPZone fungeert hierbij als het deel waarin de volledige dataset van alle infectieziekten per GGD is ondergebracht." (p. 1 en p. 14), "Daarnaast is HPZone-Lite ontwikkeld, HPZone-Lite vormt een zogenaamde 'landelijke schil'." (p. 2). In wiens opdracht HPZone Lite is ontwikkeld, heeft Dirkzwager niet kunnen achterhalen (p. 14), maar evident is dat de Staat hiertoe opdracht heeft gegeven, nu de landelijke coördinatie door het ministerie plaatsvond (**productie G.47**);

k) In een bijlage bij een adviesnota van het dagelijks bestuur van de GGD Noord- en Oost-Gelderland wordt opgesomd welke opdrachten de minister naar aanleiding va het GGD-datalek aan GGD GHOR en de GGD'en heeft gegeven: gebruik van HPZone Lite te beperken tot een selecte groep specialisten, van HPZone Lite over te stappen op een ander systeem, de print- en exportfuncties uit te schakelen, de toegangs-en zoekmogelijkheden te beperken, het monitoren van verdachte patronen en verdacht gedrag van medewerkers, het laten doorlichten van de systemen door externe IT-deskundigen, de VOG-administratie op orde brengen en het vormen van een kernteam om de GGD bij het implementeren van de maatregelen te ondersteunen (**productie G.49**).

178. Gelet op het bovenstaande stelt de Staat doel en middelen vast van de verwerking van persoonsgegevens in de systemen CoronIT en HPZone (Lite). De Staat dient derhalve als verwerkingsverantwoordelijke zoals bedoeld in artikel 4, onderdeel 7 van de AVG te worden aangemerkt. Of de Staat al dan niet feitelijke toegang tot persoonsgegevens heeft gehad, is daarvoor niet relevant.[48]

4.2.1.2 Subsidiair: (gezamenlijke) verantwoordelijkheid Staat met GGD GHOR en de GGD'en

179. Voor zover de Staat niet als zelfstandig verwerkingsverantwoordelijke wordt aangemerkt, stelt Stichting ICAM zich subsidiair op het standpunt dat GGD GHOR en de GGD'en als (gezamenlijk) verwerkingsverantwoordelijken moeten worden aangemerkt, naast de Staat.

180. 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,[49] en omdat zij het beheer heeft gevoerd over de inrichting van HPZone Lite. Ook heeft GGD GHOR HPZone Lite zodanig ingericht dat de GGD'en elkaar konden ondersteunen bij BCO. GGD GHOR presenteert zich bovendien als verwerkingsverantwoordelijke in haar communicatie, onder andere doordat zij een eigen privacyverklaring heeft en een deel van de Gedupeerden uit haar naam heeft geïnformeerd over het GDD-datalek (**producties F.16 t/m F.21**).

---

48 EDPB, 'Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG', Vastgesteld op 7 juli 2021.

49 *Kamerstukken II* 2020-2021, 27529, nr. 234, vraag 158 (**productie D.2**).

181. Ten tweede kwalificeren de 25 GGD'en als (gezamenlijk) verwerkingsverantwoordelijken, zoals ook wordt erkend door het ministerie, 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 zorgverleners waar het gaat om testen en vaccineren. Uit dien hoofde bestaat een behandelovereenkomst tussen de GGD en de Betrokkenen 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 (**productie F.16 t/m F.18**).

182. Ten derde gaan GGD GHOR en de GGD'en er zelf van uit dat zij gezamenlijk verwerkingsverantwoordelijken zijn. Dat blijkt onder andere uit het Convenant gegevensuitwisseling gezamenlijk verantwoordelijken, dat ziet op CoronIT (**productie G.30**), en het Convenant landelijke inzet BCO, dat mede ziet op HPZone Lite (**productie G.53**).

183. Ten vierde blijkt de gezamenlijke verantwoordelijkheid van GGD GHOR en de GGD'en uit een juridische analyse en documentenonderzoek dat advocatenkantoor Dirkzwager heeft uitgevoerd in opdracht van de GGD Noord- en Oost-Gelderland (**productie G.47**). Dirkzwager concludeert met betrekking tot CoronIT dat GGD GHOR "overwegend heeft te gelden als verwerkingsverantwoordelijke" en dat "de GGD'en die er gebruik van maken in beperkte mate verwerkingsverantwoordelijke zijn, en wel voornamelijk met betrekking tot de individuele verwerkingen die door de eigen GGD plaatsvinden" (p. 12). Alle betrokken verwerkingsverantwoordelijken kunnen volgens Dirkzwager "hoofdelijk aansprakelijk gesteld worden" (zie p. 13). Met betrekking tot HPZone Lite concludeert Dirkzwager dat GGD GHOR in ieder geval verwerkingsverantwoordelijke is. Weliswaar geschiedde het daadwerkelijk toegang verschaffen tot persoonsgegevens in HPZone Lite door de GGD'en, maar "zij lijken er echter feitelijk weinig invloed op te hebben aan wie zij de toegang verschaffen". Selectie van de medewerkers die toegang moesten krijgen, geschiedde door de door GGD GHOR ingehuurde callcenters en de GGD'en moesten hieraan noodgedwongen meewerken (p. 17 en 18). Dirkzwager concludeert overigens dat er geen overeenstemming lijkt te bestaan tussen hetgeen is opgenomen in het Convenant gegevensuitwisseling tussen GGD GHOR en de GGD'en (**productie G.30**) en de feitelijke gang van zaken. Ook concludeert Dirkzwager dat hetgeen GGD GHOR aan de AP heeft gecommuniceerd over de verdeling van verantwoordelijkheden, niet in overeenstemming lijkt te zijn met de werkelijkheid (p. 19). In een opvolgend advies reageert Dirkzwager op een ander advies, van privacy-consultants Hooghiemstra & Partners (dat advies is, voor zover op dit moment bekend, door geen van de Gedaagden openbaargemaakt). Daarin zou zijn geadviseerd dat GGD GHOR eigenlijk geen verwerkingsverantwoordelijke zou moeten

zijn, omdat zowel zij als de GGD'en in die situatie in strijd met de AVG zouden handelen (**productie G.48**).

4.2.1.3 Meer-subsidiair: (gezamenlijke) verantwoordelijkheid GGD GHOR, GGD'en, Gemeenten en Veiligheidsregio's

184. Voor zover geen sprake is van zelfstandige verwerkingsverantwoordelijkheid van de Staat, en GGD GHOR en de GGD'en niet als gezamenlijk verwerkingsverantwoordelijken moeten worden aangemerkt naast de Staat, stelt Stichting ICAM zich meer-subsidiair op het standpunt dat GGD GHOR en de GGD'en op grond van het bovenstaande als gezamenlijk verwerkingsverantwoordelijken moeten worden aangemerkt, samen met de Gemeenten en de Veiligheidsregio's.

185. De colleges van burgemeester en wethouders van de Gemeenten zijn op grond van de Wpg belast met het uitvoeren van taken ter bevorderingen en continuering van de publieke gezondheidszorg (zie paragraaf 2.2.5). Zij zorgen onder meer voor de instelling en instandhouding van GGD'en, financiering van die GGD'en en het houden van toezicht. Gemeenten bepalen in die hoedanigheid dan ook samen met GGD GHOR, de GGD'en zelf en de Veiligheidsregio's het doel en de middelen van de verwerking van persoonsgegevens door de GGD'en. Uit een interne mailwisseling binnen de Gemeente Rotterdam blijkt ook dat de gemeente zichzelf als verwerkingsverantwoordelijke ziet (**productie G.54**).

186. Het bestuur van de Veiligheidsregio draagt uit hoofde van artikel 6 lid 2 Wpg zorg voor de voorbereiding op de bestrijding van een epidemie die behoort tot groep A, zoals het coronavirus. De voorzitter van de Veiligheidsregio moet op grond van datzelfde artikel zorgdragen voor de bestrijding zelf. De minister kan voorzitters van de veiligheidsregio's op grond van artikel 7 Wpg instructies geven over hoe zij de bestrijding ter hand moeten nemen. De voorzitters van de 25 veiligheidsregio's maken samen het Veiligheidsberaad uit. In de eerste fase van de coronacrisis kwam het Veiligheidsberaad wekelijks samen, onder meer om te bespreken hoe invulling moest worden gegeven aan de maatregelen die het kabinet afkondigde. Het Veiligheidsberaad fungeerde als gesprekpartner voor het kabinet om van gedachten te wisselen over de benodigde maatregelen.

4.2.2 Bewijslast m.b.t. AVG-overtredingen

187. Artikel 5 lid 2 AVG bepaalt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen uit artikel 5 lid 1 AVG, waaronder de beginselen van rechtmatigheid, transparantie, minimale gegevensverwerking en integriteit en vertrouwelijkheid. De verwerkingsverantwoordelijke moet kunnen aantonen dat hij voldoet aan deze beginselen. Dit wordt de verantwoordingsplicht genoemd. De beginselen worden in de overige artikelen van de AVG uitgewerkt, waarmee de verantwoordingsplicht in wezen voor alle verplichtingen uit de AVG geldt. Dit wordt bevestigd in artikel 24 AVG, waaruit volgt dat de verwerkingsverantwoordelijke

moet kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Uit overweging 74 en 79 AVG volgt dat voor iedere verwerking vastgesteld moet worden wie de verwerkingsverantwoordelijke is en dat deze partij moet kunnen aantonen dat hij aan de AVG voldoet. Voorgaande heeft tot gevolg dat op de Staat c.s. de bewijslast rust om aan te tonen dat zij hebben voldaan aan hun verplichtingen op grond van de AVG en dat op Stichting ICAM dus geen bewijslast rust om aan te tonen dat dat niet het geval is.

4.2.3 Inbreuk in verband met persoonsgegevens / strijd met artikel 34 AVG

4.2.3.1 Inbreuk in verband met persoonsgegevens

188. De incidenten zoals beschreven in hoofdstuk 3 leveren een “inbreuk in verband met persoonsgegevens” op zoals beschreven in artikel 4, onderdeel 12 AVG en artikel 33 en 34 AVG.

189. In artikel 4, onderdeel 12 AVG wordt een inbreuk in verband met persoonsgegevens (ook wel: “datalek”) omschreven als “een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens."

190. Er is sprake geweest van een inbreuk op de beveiliging die op onrechtmatige wijze heeft geleid tot ongeoorloofde verstrekking van en toegang tot opgeslagen persoonsgegevens. Ook de Staat c.s. en de AP (**productie D.3, o.a. p. 46 en p. 68 en productie K.1**) kwalificeren de reeks incidenten als datalek.

4.2.3.2 Geen mededeling aan (alle) Betrokkenen

191. Wanneer er een datalek heeft plaatsgevonden dat waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moet een verwerkingsverantwoordelijke dat op grond van artikel 34 AVG onverwijld aan de Betrokkenen meedelen. Of er sprake is van een hoog risico moet aan de hand van de omstandigheden van het geval worden bepaald. Bij die beoordeling moet in ieder geval rekening worden gehouden met (i) de aard van de inbreuk, (ii) de aard, gevoeligheid en omvang van de persoonsgegevens, (iii) het gemak waarmee personen kunnen worden geïdentificeerd, (iv) de ernst van de gevolgen voor personen, (v) bijzondere kenmerken van de persoon, (vi) bijzondere kenmerken van de verwerkingsverantwoordelijke en (vii) het aantal getroffen personen.[50]

192. Mededeling van een datalek is niet verplicht indien (i) er passende technische en organisatorische maatregelen zijn toegepast op de persoonsgegevens (bijvoorbeeld versleuteling), (ii) de verwerkingsverantwoordelijke achteraf maatregelen heeft genomen zodat

[50] Groep gegevensbescherming artikel 29, *Richtsnoeren voor de melding in verband met persoonsgegevens krachtens Verordening 2016/679*, laatstelijk herzien en goedgekeurd op 6 februari 2018, p. 28-30.

het hoge risico zich niet meer zal voordoen of (iii) de mededeling onevenredige inspanning zou vergen. In dat laatste geval dient er een openbare mededeling te volgen waarmee betrokkenen even doeltreffend worden geïnformeerd. Van de situatie onder (iii) is bijvoorbeeld sprake als de contactgegevens van betrokkenen verloren zijn gegaan als gevolg van de inbreuk of als deze gegevens niet bekend zijn.[51]

193. Wanneer uit logbestanden met zekerheid kan worden vastgesteld dat geen sprake is geweest van exfiltratie van persoonsgegevens, kan een melding mogelijk achterwege blijven. In de Richtsnoeren 01/2021 over de voorbeelden betreffende de melding van inbreuken in verband met persoonsgegevens beschrijft de EDPB bijvoorbeeld de volgende situatie:

> "Er zijn logbestanden beschikbaar waarin alle gegevensstromen worden geregistreerd die het bedrijf verlaten (waaronder uitgaande e-mail). Nadat de logboeken en de door de detectiesystemen van het bedrijf verzamelde gegevens waren geanalyseerd, werd bij een door het externe cyberbeveiligingsbedrijf ondersteund intern onderzoek met zekerheid vastgesteld dat de dader alleen gegevens had versleuteld, zonder deze te exfiltreren. De logboeken laten geen uitgaande gegevensstroom tijdens de aanval zien." ["met zekerheid" is in de originele versie gecursiveerd, advocaat.][52]

194. De verwerkingsverantwoordelijke dient er volgens de EDPB echter rekening mee te houden dat er gegevens geëxfiltreerd kunnen zijn zonder dat daarvan een spoor is achtergelaten in de logbestanden van betrokken systemen. De verwerkingsverantwoordelijke mag zelf niet zomaar berusten bij logbestanden die in orde lijken:

> "De gegevensverwerker mag niet uit het oog verliezen dat als de aanval meer geavanceerd is, de malware de functionaliteit heeft om logbestanden te bewerken en het spoor te verwijderen. Aangezien logbestanden niet naar een centrale logserver worden doorgezonden of gerepliceerd, kan de verwerkingsverantwoordelijke zelfs na een grondig onderzoek waarbij is vastgesteld dat de persoonsgegevens door de aanvaller niet zijn geëxfiltreerd dus niet verklaren dat de afwezigheid van een vermelding in de logbestanden bewijst dat er geen exfiltratie heeft plaatsgevonden. Daarom kan een inbreuk op de vertrouwelijkheid niet geheel worden uitgesloten." [53]

195. Als voornoemde factoren voor het bepalen van het risico van een datalek worden toegepast op het GGD-datalek, blijkt evident dat het gaat om een datalek dat zeer hoge risico's met zich meebrengt voor de rechten en vrijheden van betrokkenen.

196. Voor wat betreft de aard van de inbreuk gaat het om een inbreuk waarbij (bijzondere) persoonsgegevens onbegrensd toegankelijk waren voor alle GGD-medewerkers. Bovendien

---

51 Groep gegevensbescherming artikel 29, *Richtsnoeren voor de melding in verband met persoonsgegevens krachtens Verordening 2016/679*, laatstelijk herzien en goedgekeurd op 6 februari 2018, p. 25.

52 EDPB, *Richtsnoeren 01/2021 over de voorbeelden betreffende de melding van inbreuken in verband met persoonsgegevens*, vastgesteld op 14 december 2021, par. 16.

53 EDPB, *Richtsnoeren 01/2021 over de voorbeelden betreffende de melding van inbreuken in verband met persoonsgegevens*, vastgesteld op 14 december 2021, par.19 en 28.

konden de medewerkers alle gegevens downloaden en zijn deze persoonsgegevens aan onbevoegde derden verstrekt. De aard, gevoeligheid en omvang van de bij de inbreuk betrokken persoonsgegevens is eveneens een ongunstige factor voor de Gedupeerden. Het gaat immers om een combinatie van BSN en medische gegevens:

> "Inbreuken waarbij gezondheidsgegevens, identiteitsdocumenten of financiële gegevens (bijv. creditcardgegevens) betrokken zijn, kunnen elk op zich schade veroorzaken, maar als die gegevens worden gecombineerd, kunnen ze worden gebruikt voor identiteitsdiefstal. Een combinatie van persoonsgegevens is doorgaans gevoeliger dan een enkel persoonsgegeven."[54]

197. Bovendien gaat het om NAW-gegevens, contactgegevens en BSN-nummers, waardoor een specifiek persoon direct te identificeren is voor iemand die toegang heeft tot de gecompromitteerde gegevens.

198. Het GGD-datalek heeft geleid en kan leiden tot ernstige gevolgen voor de Gedupeerden, die samenhangen met de aard van de gegevens die gelekt zijn. In de Richtsnoeren wordt daarover gemeld:

> "Afhankelijk van de aard van de bij een inbreuk betrokken persoonsgegevens, bijvoorbeeld speciale gegevenscategorieën, kan de schade voor personen die daaruit zou kunnen voortvloeien bijzonder ernstig zijn, met name als de inbreuk zou kunnen leiden tot identiteitsdiefstal of -fraude, lichamelijk letsel, psychisch leed, vernedering of reputatieschade. […] Of de verwerkingsverantwoordelijke zich er al dan niet van bewust is dat persoonsgegevens in handen zijn van personen van wie de intenties onbekend of mogelijk kwaadwillig zijn, kan van invloed zijn op het niveau van het potentiële risico."[55]

199. In het geval van het GGD-datalek ging het onder meer om gezondheidsgegevens en BSN, en zijn de kwade intenties van de mensen die de persoonsgegevens te koop aanbieden duidelijk. Er is geen sprake van een zogenaamde "betrouwbare ontvanger", zoals bijvoorbeeld een zakelijke partner waarmee een geheimhoudingsverplichting is overeengekomen, aan wie de persoonsgegevens abusievelijk zijn toegestuurd. In het geval van het GGD-datalek werden persoonsgegevens willens en wetens te koop aangeboden aan wie er maar geld voor over had.

200. De Groep gegevensbescherming artikel 29 merkt op dat wat betreft de ernst en de gevolgen ook rekening moet worden gehouden met het blijvende karakter van de gevolgen voor personen, waarbij de gevolgen als groter kunnen worden beschouwd indien het langetermijneffecten betreft. Nu sprake is van exfiltratie van persoonsgegevens die vervolgens te kwader trouw zijn aangeboden en nu circuleren op het internet, ondervinden Gedupeerden daar nog steeds de gevolgen van zoals ook beschreven in paragraaf 5.3.1.3. Het verlies van controle dat Gedupeerden hebben geleden, is naar zijn aard blijvend. Er is geen manier waarop Gedupeerden

---

54 Groep gegevensbescherming artikel 29, *Richtsnoeren voor de melding in verband met persoonsgegevens krachtens Verordening 2016/679*, laatstelijk herzien en goedgekeurd op 6 februari 2018, p. 28.

55 Groep gegevensbescherming artikel 29, *Richtsnoeren voor de melding in verband met persoonsgegevens krachtens Verordening 2016/679*, laatstelijk herzien en goedgekeurd op 6 februari 2018, p. 29.

deze controle kunnen heroveren. De indringende combinatie van persoonsgegevens maakt dat mitigerende maatregelen een zeer beperkt effect hebben.

201. De bijzondere kenmerken van Betrokkenen kunnen maken dat een inbreuk grotere risico's en/of gevaren met zich meebrengt. Daarbij kan gedacht worden aan kinderen of andere kwetsbare personen. In de GGD-systemen zitten ook veel gegevens van kwetsbare personen zoals ouderen en mensen met een verzwakte gezondheid. Bovendien zien veel gegevens op specifiek de verzwakte gezondheid. Zo bevatte CoronIT bijvoorbeeld, zoals geschetst in paragraaf 3.3.1, "*medische gegevens, om te bepalen of u een vaccinatie kunt krijgen (contra-indicaties en medische triage).*" HPZone (Lite) bevatte, zoals beschreven in paragraaf 3.3.2, gegevens als "*behoren tot medische risicogroep*", "*Sprake van gestoorde afweer*", "*huidige verblijfplaats (e.g. zorginstelling, asielzoekerscentrum […]*", "*Medische voorgeschiedenis [welke ziektes heeft index gehad of momenteel]*".

202. Verder zijn ook de bijzondere kenmerken van de verwerkingsverantwoordelijke relevant voor het bepalen van het risico welke een inbreuk met zich meebrengt:

> "Zo zal een medische organisatie speciale categorieën van persoonsgegevens verwerken, wat betekent dat er een grotere bedreiging is voor personen als hun persoonsgegevens zijn geschonden dan bij een mailinglijst van een krant."[56]

203. In het geval van het GGD-datalek gaat het om de overheid als verwerkingsverantwoordelijke. De overheid verwerkt op grote schaal persoonsgegevens van burgers, waar zij veelal verplicht mee akkoord dienen te gaan. Burgers moeten dan ook in het bijzonder op de overheid kunnen vertrouwen om persoonsgegevens adequaat te beveiligen. Daarnaast gaat het in onderhavige zaak om medische organisaties die bijzondere persoonsgegevens verwerken.

204. Wat betreft het aantal personen dat is getroffen merkt de Groep gegevensbescherming artikel 29 op:

> "Een inbreuk kan slechts één persoon treffen of kan een paar personen, enkele duizenden personen of nog veel meer personen treffen. Over het algemeen kan een inbreuk grotere gevolgen hebben naarmate er meer personen bij betrokken zijn."[57]

205. In dit geval zijn er zeker 6,5 miljoen Gedupeerden.

206. Uit voorgaande volgt dat de Staat c.s. het datalek ten onrechte niet rechtstreeks aan alle Gedupeerden hebben gemeld. Ook de FAQ op de website van GGD GHOR geeft er blijk van dat de Staat c.s. artikel 34 AVG hebben geschonden. Daarin staat bijvoorbeeld: "*Tot nu toe is uit*

---

[56] Groep gegevensbescherming artikel 29, *Richtsnoeren voor de melding in verband met persoonsgegevens krachtens Verordening 2016/679*, laatstelijk herzien en goedgekeurd op 6 februari 2018, p. 29.

[57] Groep gegevensbescherming artikel 29, *Richtsnoeren voor de melding in verband met persoonsgegevens krachtens Verordening 2016/679*, laatstelijk herzien en goedgekeurd op 6 februari 2018, p. 30.

politieonderzoek alleen gebleken dat er uit CoronIT gegevens gestolen zijn" en "*We hebben vernomen dat datasets worden aangeboden, maar hebben nog niet kunnen vaststellen dat deze feitelijk verhandeld zijn*.". Uit de uitleg van de EDPB blijkt echter dat in het geval een inbreuk heeft plaatsgevonden die waarschijnlijk een hoog risico inhoudt, melding aan betrokkenen slechts dan mogelijk achterwege kan blijven als exfiltratie van gegevens met zekerheid uitgesloten kan worden. Als dat niet het geval is, moeten alle Betrokkenen rechtstreeks geïnformeerd worden.

207. Nu volledige logbestanden ontbreken (paragraaf 4.2.4.4), hadden de Staat c.s. niet slechts die beperkte groep moeten informeren die na onderzoek door de politie zijn geïdentificeerd, maar alle Gedupeerden, per brief of e-mail, en onverwijld. Nu uit de loggegevens niet met zekerheid is af te leiden welke gegevens daadwerkelijk onrechtmatig zijn geëxporteerd (zie paragraaf 3.4), bestaat de groep Gedupeerden aan wie een melding had moeten worden gedaan uit zeker 6,5 miljoen personen en niet uit 1.250.

208. Bovendien hebben de Staat c.s. geen tijdige melding gedaan aan de 1.250 Gedupeerden die wel zijn geïnformeerd. Zoals blijkt uit hoofdstuk 3, kwamen al in september 2020 de eerste berichten in de pers over een datalek bij de GGD´en. Het callcenterbedrijf Teleperformance heeft omstreeks die periode al een melding gedaan bij de AP ten aanzien van te ruime autorisaties van callcentermedewerkers die na uitdiensttreding nog steeds toegang hadden tot de systemen (**productie C.3**). In november 2020 werd door de Volkskrant naar buiten gebracht dat GGD GHOR er al in juni 2020 mee bekend was dat HPZone niet geschikt was voor gebruik voor grootschalige epidemieën (**productie C.5**). Op 25 januari 2021 berichtte RTL Nieuws over chatdiensten waarop al maanden persoonsgegevens te koop waren aangeboden. Een paar dagen daarvoor, op 22 januari 2021 is, zoals blijkt uit het onderzoek van de AP, het datalek pas door GGD GHOR gemeld aan de AP.

209. Uit de brief van de AP volgt dat er tussen 25 januari en 29 januari 2021 meermaals contact is geweest tussen de AP en GGD GHOR over de kennisgeving richting Betrokkenen op grond van artikel 34 AVG. De GGD heeft op 28 januari 2021 op haar website informatie verstrekt over het datalek (**producties F.5**). Vanaf 16 april 2021 zijn de 1.250 Gedupeerden waarvan de politie heeft vastgesteld dat daadwerkelijk persoonsgegevens zijn gestolen per brief geïnformeerd over het datalek (**productie F.20**). Dat is dus geruime tijd na de melding die GGD GHOR aan de AP gedaan heeft. Dat terwijl artikel 34 AVG vereist dat de verwerkingsverantwoordelijke, wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, die inbreuk onverwijld aan de Betrokkenen meldt.

210. Voor zover de AP op grond van artikel 34 lid 4 AVG heeft besloten dat de melding die GGD GHOR op de website heeft geplaatst voldoende was in de zin van artikel 34 lid 3 is dit lastig te volgen in het licht van het voorbeeld van de voorganger van de EDPB over het ondergelopen magazijn van het bureau voor de statistiek dat enkel persoonsgegevens bevatte op papier. De Staat c.s. hadden juist de contactgegevens van alle Gedupeerden goed in kaart, omdat met hen gecommuniceerd

werd over testuitslagen etc. Het GGD-datalek heeft nooit de beschikbaarheid van gegevens aangetast.

4.2.4 Schending van de beveiligingsplicht (artikel 5 lid 1 sub f AVG en artikel 32 AVG)

211. Gezien de grootschalige verwerking van gevoelige en bijzondere persoonsgegevens was de beveiliging door de Staat c.s. niet passend, zoals bedoeld in artikel 32 AVG. Gegevens waren toegankelijk voor onbevoegde personen. (Ex-)medewerkers van GGD'en en landelijke partners hebben zonder dat dit werd gesignaleerd of kon worden gesignaleerd persoonsgegevens kunnen exporteren en voor eigen (criminele) doeleinden kunnen gebruiken. Reeds het enkele feit dat dit plaats kon vinden, geeft blijk van onvoldoende beveiliging. De maatregelen die de Staat c.s. daartegen hadden kunnen en moeten nemen waren bovendien basaal en eenvoudig voorhanden, ook in ogenschouw nemende de stand van de techniek en de uitvoeringskosten. Het gebrek aan deze maatregelen heeft geleid tot een groot, ernstig en gerealiseerd risico voor de rechten en vrijheden van Betrokkenen. De Staat c.s. hebben het daadwerkelijk ongeoorloofd doorzoeken, exporteren en printen van persoonsgegevens uit de systemen niet weten te voorkomen.

212. In deze paragraaf zal uitgebreider worden beschreven hoe de algemene norm van artikel 5 lid 1 sub f en artikel 32 AVG wordt uitgelegd (paragraaf 4.2.4.1) en op welke punten de Staat c.s. deze hebben geschonden. De Staat c.s. hebben in het bijzonder onvoldoende maatregelen genomen op het gebied van toegangsbeveiliging (paragraaf 4.2.4.2), autorisaties (paragraaf 4.2.4.3), logging en monitoring (paragraaf 4.2.4.4) en screening en toezicht (paragraaf 4.2.4.5). Hierbij wordt zoveel mogelijk de structuur gehanteerd van de brief van de AP naar aanleiding van haar onderzoek bij GGD GHOR en twee GGD'en (**productie K.1**). Hier wordt herhaald dat het onderzoek van de AP slechts heel beperkt is geweest (zie verder paragraaf 3.1.9).

4.2.4.1 Algemeen toetsingskader

213. Artikel 5 lid 1 sub f AVG bevat het beginsel van vertrouwelijkheid en integriteit van persoonsgegevens. Het beginsel omvat bescherming tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging, door middel van passende technische en organisatorische maatregelen.

214. 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, "*rekening houdend met de stand van de techniek, de uitvoeringskosten, de aard, de omvang, de context en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen*". Ingevolge het tweede lid wordt bij de beoordeling van het passende beveiligingsniveau met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de

ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

215. Een op het risico afgestemd beveiligingsniveau omvat onder meer het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen (artikel 32 lid 1 sub b AVG) en een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking (artikel 32 lid 1 sub d AVG).

216. De AP heeft herhaaldelijk aangegeven dat NEN 7510, 7512 en 7513 als algemeen geaccepteerde beveiligingsstandaarden onder het AVG-regime een belangrijke norm voor informatiebeveiliging in de zorg zijn en dat deze richtlijnen gevolgd moeten worden, zoals in de Richtsnoeren Beveiliging van Persoonsgegevens,[58] op haar website (**productie K.21**) en in handhavingstrajecten.[59] De AP gebruikt NEN 7510, 7512 en 7513 dan ook als norm bij de toetsing van de door artikel 32 AVG voorgeschreven passende technische en organisatorische maatregelen"[60] De AP bevestigde ook in haar brief van 8 november 2021 dat deze normen van toepassing zijn op de verwerking van persoonsgegevens in de GGD-systemen (**productie K.1**).[61]

217. In een zaak tussen het Haga-ziekenhuis en de AP bevestigde de rechtbank Den Haag dat NEN-normen algemeen geaccepteerde beveiligingsstandaarden zijn binnen de praktijk van de informatiebeveiliging in de zorg. Dat blijkt ook uit de vastlegging daarvan in het Begz. NEN-normen kunnen dan ook gebruikt worden ter invulling van de open norm van artikel 32 AVG, waaronder ten aanzien van de verplichting tot (controle op) logging.[62] Recent heeft ook de rechtbank Zeeland-West-Brabant in een zaak tegen het Bravis-ziekenhuis bevestigd dat de invulling van artikel 32 AVG plaatsvindt aan de hand van de NEN 7510 en 7513.[63]

218. Een algemene beveiligingsnorm waarbij de AP aansluit voor de beoordeling of sprake is van passende technische en organisatorische beveiligingsmaatregelen is de Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2017), waarin internationaal geldende maatregelen voor informatiebeveiliging zijn uitgewerkt. Deze norm ziet niet specifiek op de zorg. De normen

---

58 CBP Richtsnoeren: Beveiliging van persoonsgegevens, *Stcrt*. 2013, 5174. Hoewel de richtsnoeren nog uit 2013 dateren, zijn deze onder de AVG nog steeds relevant aangezien er geen (wezenlijke) wijzigingen zijn ten aanzien van de beveiligingsplicht onder de AVG ten opzichte van de Wet bescherming persoonsgegevens. De richtsnoeren zijn grotendeels gebaseerd op nog steeds geldende beveiligingsstandaarden binnen het vakgebied informatiebeveiliging.

59 Autoriteit Persoonsgegevens, 'Toegang tot digitale patiëntdossiers door medewerkers van het HagaZiekenhuis', Onderzoeksrapport maart 2019, p. 6.

60 Autoriteit Persoonsgegevens, 'Besluit tot het opleggen van een bestuurlijke boete aan OLVG', 26 november 2020.

61 Zie verder paragraaf 4.3.2 ten aanzien van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en het Besluit elektronische gegevensverwerking door zorgaanbieders.

62 Rechtbank Den Haag 31 maart 2021, ECLI:NL:RBDHA:2021:3090 (*Haga-ziekenhuis/AP*).

63 Rechtbank Zeeland-West-Brabant, 21 september 2022, ECLI:NL:RBZWB:2022:5457 (*X/Bravis Ziekenhuis*), r.o. 4.14.

in de Code voor Informatiebeveiliging zijn echter voor het grootste deel gelijk van inhoud aan de normen in de NEN-normen. Tenzij anders vermeld, worden in het onderstaande telkens slechts de NEN-normen besproken, waarbij dus wordt opgemerkt dat hetzelfde geldt onder de Code voor Informatiebeveiliging.

219. Gezien de omvang en algemene bekendheid van de NEN-normen en de Code voor Informatiebeveiliging heeft Stichting ICAM ervoor gekozen deze niet in het geding te brengen, maar hieruit te citeren. Zij biedt echter hierbij aan deze stukken alsnog in het geding te brengen indien de rechtbank dat wenst.

4.2.4.2 Toegangsbeveiliging: authenticatie, toegang en thuiswerken

220. Het voorkomen van ongeoorloofde toegang en het implementeren en uitvoeren van een goed authenticatieproces zijn essentiële aspecten van de beveiliging van persoonsgegevens en het waarborgen van een passend beschermingsniveau. Ook de wijze waarop door geoorloofde gebruikers toegang wordt verkregen tot persoonsgegevens dient te voldoen aan bepaalde standaarden. Wanneer gebruikers bijvoorbeeld via onbeveiligde of ongecontroleerde verbindingen toegang kunnen verkrijgen, kunnen daarmee bepaalde beveiligingsmaatregelen worden omzeild of kunnen ongezien ongeoorloofde handelingen worden verricht.

221. De NEN 7510 omschrijft welke beheers- en implementatiemaatregelen genomen moeten worden in het kader van authenticatie, toegang en telewerken, waaronder de volgende:

a) Ten eerste dient een beleid voor toegangsbeveiliging en -controle te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen dat aan bepaalde eisen dient te voldoen. Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren de toegang tot die informatie te controleren. In het algemeen behoren gebruikers van gezondheidsinformatiesystemen de toegang tot persoonlijke gezondheidsinformatie te beperken tot situaties waarin er een zorgrelatie bestaat tussen de gebruiker en de betrokkene, waarin de gebruiker een activiteit uitvoert namens de betrokkene en waarin specifieke gegevens nodig zijn om deze activiteit te ondersteunen. De organisatie behoort alle partijen te identificeren en documenteren waarmee gegevens worden uitgewisseld, en met deze partijen behoren contractuele afspraken over toegang en rechten te worden gemaakt, alvorens gegevens uit te wisselen;[64]

b) Ten tweede dienen bij telewerken (thuiswerken) beleid en ondersteunende beveiligingsmaatregelen te worden vastgesteld en geïmplementeerd ter beveiliging van gegevens die worden verwerkt vanaf telewerklocaties, zoals ten aanzien van het voorkomen van de opslag van gegevens op privéapparatuur en het voorkomen van onbevoegde toegang, zoals door bijvoorbeeld familie en vrienden. Daarbij dient onder

[64] NEN 7510-2:2017, paragraaf 9.1.1, p. 44 e.v.

andere rekening te worden gehouden met de gevoeligheid van de informatie en de vraag of informatie opgeslagen moet kunnen worden op eigen apparatuur;[65]

c) Ten derde dienen beveiligingsmaatregelen in acht te worden genomen ten aanzien van apparatuur die zich buiten het bedrijfsterrein bevindt en waarop gegevens worden verwerkt. Gebruik van dergelijke apparatuur dient onder andere door de directie te worden goedgekeurd. Ook dienen er afspraken te worden vastgelegd over de fysieke beveiliging van dergelijke apparatuur. Verder dient onderwerpspecifiek beleid te worden vastgesteld ter zake beveiligde configuratie en beveiligd gebruik daarvan. Het beleid dient onder andere in aanmerking te nemen: de registratie van de eindapparatuur, beperkingen van de installatie van software, regels voor updates, toegangsbeveiliging, versleuteling, analyse van het gedrag van de eindgebruiker en het gebruik van externe opslagapparaten zoals USB-sticks. Wanneer wordt gewerkt met zeer gevoelige gegevens, dient te worden overwogen om het onmogelijk te maken om gegevens op te slaan op de eindapparatuur zelf. Wanneer gebruikt wordt toegestaan van eigen apparatuur, gelden nog aanvullende vereisten, zoals regels over scheiding van zakelijk en privégebruik en het bevestigen door de gebruikers van hun verplichtingen. Er dient bij dit alles rekening te worden gehouden met de vraag of de apparatuur alleen binnen de beveiligde omgeving van de organisatie wordt gebruikt of ook daarbuiten.[66]

222. De AP heeft op 8 november 2021 geconcludeerd dat de toegangsbeveiliging op de GGD-systemen onvoldoende was (**productie K.1)**. De GGD-systemen konden vanaf eigen apparatuur rechtstreeks worden benaderd via een URL buiten de beveiligde werkomgeving. Ook is gebleken dat laptops werden verstrekt aan een deel van de medewerkers, terwijl een andere groep medewerkers, waaronder medewerkers van de landelijke partners, op eigen apparatuur werkte. Hiervoor is geen eenduidig beleid aangetroffen. Bovendien heeft GGD GHOR aangegeven met de landelijke partners geen afspraken te hebben vastgelegd over het werken op eigen apparatuur.

223. De AP heeft opgemerkt dat het gebruik van eigen apparatuur in combinatie met de mogelijkheid om op de onderzochte systemen in te loggen buiten een beveiligde werkomgeving, kan leiden tot beveiligingsrisico's. Omdat de eigen apparatuur niet in beheer is bij de werkgever, is niet bekend of de apparatuur aan bepaalde beveiligingseisen voldoet en is het niet mogelijk om bepaalde technische beveiligingsmaatregelen te implementeren.

224. Er bestond dus geen beleid ten aanzien van het opslaan van persoonsgegevens op eigen apparatuur, zoals omvangrijke databestanden die konden worden geëxporteerd vanuit HPZone Lite.

[65] NEN 7510-2:2017, paragraaf 6.2.2, p. 22 e.v.
[66] NEN 7510-2:2017, paragraaf 11.2.6, p. 77 e.v. en Code voor Informatiebeveiliging, paragraaf 8.1, p. 112 e.v.

225. De risico's ten aanzien van thuiswerken op eigen apparatuur werden al geconstateerd in de BCO-DPIA van november 2020, maar zijn vervolgens dus niet opgelost (**productie G.15**):

> "Medewerkers werken thuis, wat betekent dat andere personen aanwezig kunnen zijn en gebruik kunnen maken van het thuisnetwerk. Dit betekent dat huisgenoten onrechtmatig gegevens kunnen horen of zien, indien de medewerker werkt op een locatie waar andere aanwezig zijn. Daarnaast kunnen mensen die op hetzelfde netwerk werken, toegang krijgen tot de gegevens die via dat netwerk worden verstuurd. Hierdoor kan onrechtmatige inzage van gegevens mogelijk zijn. Ten slotte gebruiken medewerkers eigen apparatuur om de werkzaamheden op uit te voeren. Medewerkers kunnen bestanden met vertrouwelijke informatie downloaden uit de beveiligde omgeving en niet/niet tijdig verwijderen. Indien deze apparatuur niet goed is beveiligd, kan worden meegekeken in de systemen van de medewerker of kunnen inloggegevens worden gestolen. Dit betekent dat fraude kan worden gepleegd met deze gegevens.
>
> - De kans dat het risico zich manifesteert is hoog. Medewerkers werken thuis, maar vaak ook de huisgenoten. Dit betekent dat de medewerker zich altijd zal moeten afzonderen, wat voor sommige medewerkers niet mogelijk is. Ook kan een huisgenoot binnenlopen bij een gesprek. Vaak wordt door huisgenoten ook hetzelfde wifi-netwerk gebruikt, waardoor deze toegang kunnen krijgen tot de data-uitwisseling van de medewerker met het netwerk.
> - De impact van het risico is hoog. Hoewel het gaat om huisgenoten, kunnen zij de persoonsgegevens opvangen. Hierdoor bestaat de kans dat wordt gesproken over de casus. Als een huisgenoot de data-uitwisseling kan volgen, betekent dat dat hij met de persoonsgegevens kan doen wat hij wenst, terwijl het hier gaat om gegevens die gevoelig zijn en die gebruikt/verkocht kunnen worden om fraude mee te plegen."

226. In een planbeschrijving van GGD Haaglanden dat ziet op de veiligheid van de GGD-systemen wordt opgemerkt dat toegang tot HPZone (Lite) slecht is bewaakt en zwakke toegangsbeveiliging kent en dat er bij CoronaIT sprake is van "Toegang tot grootschalige data- alles voor iedereen inzichtelijk" (**productie G.9**).

227. Uit voorgaande volgt dat de Staat c.s. ten aanzien van het onderwerp toegangsbeveiliging geen passend beschermingsniveau hebben geboden, in strijd met artikel 5 lid 1 sub f AVG en artikel 32 AVG.

4.2.4.3 Toegangsbeveiliging: autorisaties en toegangsrechten

228. Autorisatie is het proces waarin een persoon bepaalde aan hem of haar toegekende rechten krijgt binnen een systeem. Het doel hiervan is dat medewerkers enkel toegang hebben tot persoonsgegevens of functionaliteiten die noodzakelijk zijn voor de uitvoering van hun werk, en dat zij die toegang weer verliezen op het moment dat zij die niet langer nodig hebben. Autorisaties en het juiste beheer daarvan dragen bij aan een passend beveiligingsbeleid binnen een organisatie.

229. De NEN 7510 omschrijft welke beheers- en implementatiemaatregelen genomen moeten worden in het kader van autorisaties, waaronder de volgende:

a) Ten eerste behoren passende regels voor toegangsbeveiliging, toegangsrechten en toegangsbeperkingen voor specifieke gebruikersrollen te worden vastgesteld, waarbij de details en striktheid een afspiegeling zijn van de gerelateerde beveiligingsrisico's. Het beleid dient onder andere rekening te houden met de specifieke beveiligingseisen en de beleidsregels voor informatieautorisaties, zoals de "need-to-know" en "need-to-use" principes, met eisen voor het periodiek beoordelen van toegangsrechten, met het intrekken van toegangsrechten en met rollen met specifieke toegangsrechten. Toegangsrechten dienen te worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden, passend bij de behoeften van die rollen. Ook dienen toegangsregels te worden vastgesteld op basis van het principe "alles is in principe verboden tenzij het uitdrukkelijk is toegestaan";[67]

b) Ten tweede behoren gebruikers alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. Het daarvoor vereiste beleid dient autorisatieprocedures te omvatten om vast te stellen wie toegang krijgt en een procedure voor het monitoren van netwerkdiensten;[68]

c) Ten derde dient er een formele registratie- en afmeldingsprocedure te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. De gebruikersregistratiegegevens behoren regelmatig te worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is. De procedure behoort te omvatten: het gebruik van unieke gebruikersidentificaties zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gehouden voor hun acties (het gebruik van groepsidentificaties behoort alleen te worden toegelaten als deze om bedrijfs- of operationele redenen noodzakelijk zijn), het onmiddellijk ongeldig maken of verwijderen van gebruikersidentificaties van gebruikers die de organisatie hebben verlaten en het periodiek identificeren en verwijderen van overbodige gebruikersidentificaties, het ervoor zorgen dat overtollige gebruiksidentificaties niet aan andere gebruikers worden uitgegeven en het nauwkeurig vastleggen van de identiteit en beroepsgegevens van de gebruikers;[69]

d) Ten vierde dient er een formele gebruikerstoegangsverleningsprocedure te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. De procedure voor het toewijzen of intrekken van toegangsrechten behoort te omvatten: het verkrijgen van autorisatie van de eigenaar van het informatiesysteem, het verifiëren dat het verleende toegangsniveau in overeenstemming is met de beleidsregels voor toegang, het waarborgen dat toegangsrechten niet worden geactiveerd voordat de autorisatieprocedures zijn afgerond, het bijhouden van een centraal overzicht van toegangsrechten die aan

67 NEN 7510-2:2017, paragraaf 9.1.1, p. 45 e.v.
68 NEN 7510-2:2017, paragraaf 9.1.2, p. 47 e.v.
69 NEN 7510-2:2017, paragraaf 9.2.1, p. 48 e.v.

gebruikers zijn toegekend, het aanpassen van toegangsrechten van gebruikers wiens rollen of functies zijn gewijzigd en het onmiddellijk verwijderen of blokkeren van toegangsrechten van gebruikers die de organisatie hebben verlaten. In de procedures dient voorts duidelijk te worden vastgesteld of gebruikers al dan niet toegang krijgen tot persoonlijke gezondheidsinformatie;[70]

e) Ten vijfde behoren eigenaren van bedrijfsmiddelen de toegangsrechten van gebruikers regelmatig te beoordelen. Daarbij dient onder andere in overweging te worden genomen dat toegangsrechten regelmatig behoren te worden beoordeeld na wijzigingen, zoals beëindiging van het dienstverband;[71]

f) Ten zesde behoren de toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen te worden aangepast;[72]

g) Ten zevende behoren toegang tot informatie en systeemfuncties van toepassingen te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging. De systemen behoren de identiteit van de gebruiker vast te stellen door middel van twee-factor-authenticatie. Ook dienen de volgende aspecten in overweging te worden genomen: er moet worden beheerst welke gegevens voor een bepaalde gebruiker toegankelijk zijn, de toegangsrechten van gebruikers moeten worden beheerst, bijv. lezen schrijven, verwijderen en uitvoeren, en de informatie in output dient te worden beperkt.[73]

Geen (adequaat) toegangs- en autorisatiebeleid

230. Op basis van NEN 7510 hadden de Staat c.s. een autorisatieproces moeten hebben op basis waarvan medewerkers enkel toegang kregen tot persoonsgegevens die noodzakelijk waren voor de uitvoering van hun taken. De Staat c.s. hadden passende regels voor toegangsbeveiliging, -rechten en -beperkingen voor specifieke gebruikersrollen vast moeten stellen, waarbij de details en de striktheid van de beheersmaatregelen een afspiegeling zijn van de gerelateerde informatiebeveiligingsrisico's. Concreet betekent dit dat de Staat c.s. rollen met bijbehorende autorisaties hadden moeten vaststellen en toepassen. Die autorisaties behoren "passend" te zijn. Dat betekent dat (de noodzaak voor) de toegang tot persoonsgegevens en de beperkingen van de toegang afhankelijk zijn van de rol van de medewerker en de relatie tot de Betrokkene, waarbij

[70] NEN 7510-2:2017, paragraaf 9.2.3, p. 49 e.v.
[71] NEN 7510-2:2017, paragraaf 9.2.5, p. 53 e.v.
[72] NEN 7510-2:2017, paragraaf 9.2.6, p. 54 e.v.
[73] NEN 7510-2:2017, paragraaf 9.4.1, p. 57 e.v.

de goede uitvoering van de taken die worden uitgevoerd door de medewerker in aanmerking worden genomen.[74]

231. De AP heeft tijdens haar onderzoek in 2021 geen toereikende documentatie aangetroffen die ten aanzien van HPZone (Lite) inzichtelijk maakt welke specifieke rechten en functionaliteiten aan verschillende rollen waren gekoppeld (**productie K.1**).

232. In een concept-DPIA vaccinaties van 15 januari 2021 staat echter ook ten aanzien van CoronIT beschreven dat er geen adequaat autorisatiebeleid is opgesteld (**productie G.16**):

> "12. Toegang tot persoonsgegevens onvoldoende geregeld
> In CoronIT worden veel gegevens verwerkt en veel medewerkers met verschillende rollen hebben toegang tot (delen van) deze gegevens. De rollen moeten duidelijk zijn en wanneer bepaalde personen geen toegang nodig hebben tot bepaalde gegevens voor de uitvoering van de werkzaamheden, moet toegang tot deze gegevens worden afgeschermd. Op dit moment is daarvoor geen adequaat autorisatiebeleid opgesteld. Daarnaast lijkt de in- en uitstroom van medewerkers bij de GGD'en en verwerkers erg hoog te zijn, waardoor medewerkers wel worden aangemeld, maar niet direct worden afgemeld, waardoor ze toegang behouden tot de (medische) gegevens in CoronIT. Toegang tot persoonsgegevens lijkt onvoldoende te zijn geregeld, waardoor onbevoegden gegevens in kunnen zien. Dit leidt tot imagoschade, negatieve publiciteit en financiële schade in de vorm van boetes/sancties."

233. In de Woo-stukken heeft Stichting ICAM eveneens geen autorisatiematrixen of -procedures aangetroffen die enige betekenisvolle informatie geven, niet voor HPZone (Lite) en niet voor CoronIT. De matrixen die wel openbaar zijn gemaakt, zijn bovendien ofwel niet gedateerd ofwel van een datum na 25 januari 2021. De eerste opzet van een beleid- en procesbeschrijving voor toegangsbeveiliging van GGD Gelderland-Zuid dateert pas van 30 januari 2021, aldus van na bekendwording van het GGD-datalek (**productie G.20**). Ten aanzien van GGD IJsselland dateert de eerste versie van het Beleid Logische Toegangsbeveiliging pas van 26 november 2021 (**productie G.22**). Een Protocol Toegangs- en autorisatiebeheer Applicaties Coronaketen werd door GGD IJsselland pas definitief vastgesteld op 9 september 2021 (**productie G.23**).

234. In een memo van 30 april 2021 over het opstellen van autorisatiematrices voor HPZone (Lite) staat beschreven dat HPZone (Lite) diverse rollen kent met daaraan gekoppelde functionaliteiten, maar dat de beschrijving van die functionaliteiten niet of slechts in geringe mate beschikbaar is (**productie G.4**). Ook was er helemaal geen autorisatiematrix vanuit de leverancier of vanuit GGD GHOR bekend. Deze situatie was volgens het memo in februari 2021 aanleiding om het opstellen van een autorisatiematrix voor HPZone (Lite) op de agenda te zetten. Vanwege de vervanging van HPZone (Lite) door GGD Contact en het BCO-portaal, wordt in het memo uiteindelijk geconcludeerd dat een autorisatiematrix voor HPZone (Lite) "*op dit moment niets meer toe*

[74] Zie ook: Autoriteit Persoonsgegevens, 'Onderzoeksrapport Toegang tot digitale patiëntdossiers door medewerkers van het HagaZiekenhuis', maart 2019, p. 9.

[voegt] op het gebied van privacy, security". De GGD Haaglanden "*werkt immers al jaren met HPZone zonder al te grote incidenten*" (**productie G.4**).

235. Stichting ICAM kan daardoor niet anders concluderen dan dat er geen (afdoende) autorisatiematrixen bestaan, en dat die in ieder geval niet bestonden voorafgaand aan de berichtgeving door RTL Nieuws in januari 2021.

Toekenning van rechten was te ruim

236. De toekenning van toegangs- en gebruiksrechten binnen CoronIT en HPZone Lite was te ruim. GGD-medewerkers hadden toegang tot gegevens in de GGD-systemen (ook van andere GGD-regio's) waar zij geen toegang tot zouden moeten hebben. Ook hadden alle tienduizenden GGD-medewerkers toegang tot zowel de zoekfunctionaliteiten als de print- en exportfunctionaliteiten en hadden ongelimiteerde mogelijkheden om gegevens op te zoeken, te downloaden en te printen. Voor de uitvoering van de werkzaamheden was het niet noodzakelijk dat de betreffende functionaliteiten binnen CoronIT en HPZone Lite algemeen toegankelijk waren voor alle medewerkers. Slechts een handvol personen had die toegang nodig.

237. GGD-medewerkers hebben bevestigd dat zij toegang hadden tot gegevens in de GGD-systemen (van andere GGD-regio's) waar zij geen toegang tot zouden moeten hebben (**productie C.8**).

238. Volgens GGD GHOR hebben in CoronIT medewerkers inderdaad landelijk toegang tot alle dossiers.[75] Dat de toekenning van rechten in de GGD-systemen te ruim was, is ook door de minister erkend.[76] De AP heeft bij de twee door haar onderzochte GGD'en ook geconstateerd dat medewerkers over autorisaties beschikten die zij voor hun werkzaamheden niet of niet langer nodig hadden. Zo was de exportfunctionaliteit in HPZone Lite, waarmee grote hoeveelheden persoonsgegevens in bulk konden worden gedownload, toegankelijk voor alle reguliere rollen[77] en dus voor alle circa 20.000 (deels extern ingehuurde) GGD-medewerkers.[78]

239. Dat de rechtenverlening te ruim was, blijkt ook uit verschillende Woo-stukken.

240. In de CoronIT-referentie-DPIA is vastgesteld dat er in CoronIT geen scheiding is aangebracht van toegang tussen GGD'en, hetgeen als hoog risico wordt geclassificeerd (**productie G.1**):

> "3. Geen scheiding van toegang tussen regio's
> Voor medewerkers van GGD'en is geen scheiding aangebracht tussen de regio's in CoronIT. Dit betekent dat medewerkers van de ene regio gegevens van betrokkenen in een andere regio kunnen opzoeken. Deze keuze is gemaakt op vraag van een aantal GGD'en, omdat mensen zich buiten hun regio kunnen laten testen en voor toegang tot die gegevens dan telkens een aanvraag moet worden

75 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 9 (**productie D.2**).
76 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 17 (**productie D.2**).
77 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 9 (**productie D.2**).
78 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 39 (**productie D.2**).

ingediend, wat het proces vertraagd. Hierdoor is het echter mogelijk om onrechtmatig inzage te verkrijgen in de gegevens van alle inwoners van Nederland.

- De kans dat het risico zich manifesteert is groot. Er zijn veel medewerkers van GGD'en en ingehuurd personeel die gehele of beperkte toegang hebben tot CoronIT. De kans dat een van deze medewerkers zich, kwaadwillend of niet, toegang verschaft tot de gegevens.
- De impact van het risico is hoog. In CoronIT zijn medische gegevens en het BSN opgenomen, alsook contactgegevens. Hier kan op verschillende wijze misbruik van worden gemaakt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Besloten is dat het niet mogelijk is om CoronIT enkel voor de regio beschikbaar te stellen, omdat mensen zich ook regelmatig buiten de regio laten testen. Regel daarom dat, indien een dossier van iemand buiten de regio wordt geopend, breaking-the-glass is ingevoerd waarbij een reden moet worden ingegeven waarom de medewerker zich toegang wil verschaffen tot het dossier.
- Stel logging in op de breaking-the-glass inzages en controle elke toegang die via breaking-the-glass is verkregen. Op deze wijze kan worden beoordeeld of een medewerker rechtmatig inzage heeft gehad in de gegevens.
- Indien wordt gekozen breaking-the-glass niet in te stellen, dient strenge logging te worden toegepast op de verwerkingen in CoronIT.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Middel

Het restrisico na genomen maatregelen is dat als breaking-the-glass of een andere vorm van scheiding tussen regio's niet wordt aangezet en gecontroleerd, medewerkers toch onrechtmatig dossiers inzien uit andere regio's en de gegevens misbruiken. De medewerkers werken in een groot deel van de gevallen thuis (in het geval van het callcenter. Medewerkers van de GGD en in de teststraten werken vaker op locatie), waardoor ook geen onderling toezicht op de werkvloer bestaat. Logging kan daarbij niet iedere medewerker en iedere toegang tot de gegevens controleren."

241. Ten aanzien van CoronIT heeft GGD GHOR wel een toelichting bij de verschillende rollen opgesteld (**productie G.24**). Dit document dateert van 18 mei 2020. Daaruit blijkt dat GGD-medewerkers nagenoeg onbeperkte toegangsrechten hadden:

"De GGD-medewerker kan een aantal rollen toebedeeld krijgen.
Voor alle rollen uitgezonderd roosterplanner geldt:
• Inzicht in dossier client. Zoekfuncties naar het dossier van cliënten o.b.v. patiëntnummer, BSN, of een combinatie van twee andere persoonscriteria. Bij het openen van een dossier dat aan een andere GGD is gekoppeld wordt een 'breaking the glass'-methode toegepast, waarbij de gebruiker een reden op moet geven voordat het dossier wordt geopend.
• Inzicht in afsprakenoverzicht. Omdat GGD'en elkaar ondersteunen en werk uitwisselen (in het kader van hun WPG-taken) kunnen afspraken van andere afnamelocaties worden ingezien. Dat is nodig omdat mensen ook buiten hun woongebied getest worden. In de werkinstructies wordt duidelijk aangegeven, welke filters het best gebruikt kunnen worden om de voor de gebruiker optimale selectie zichtbaar te maken."

242. De genoemde "*breaking the glass*"-methode is echter volgens een e-mailwisseling van de gemeente Rotterdam van 1 februari 2021 nooit toegepast (**productie G.41**).

243. Uit een e-mailwisseling van 25 mei 2020 waarin een overleg tussen GGD GHOR en GGD Rotterdam-Rijnmond over privacy ten aanzien van CoronIT wordt samengevat, blijkt dat al op dat moment het bewustzijn bestond dat sprake was van te ruime toegang. Eerder zou de toegang van GGD-medewerkers tot de systemen beperkt zijn geweest tot de betreffende regio waarvoor de betreffende medewerker werkzaam is. Ten tijde van deze e-mailwisseling was de toegang, eenmaal toegekend, echter landelijk. Opgemerkt wordt dat men de "*huidige brede toegang niet proportioneel [vindt] aan het gestelde doel*" (**productie G.25**).

244. Uit de e-mailwisseling van de gemeente Rotterdam van 1 februari 2021 blijkt eveneens dat de toegang tot de GGD-systemen veel te ruim was (**productie G.41**):

> "Iedereen die toegang heeft [tot CoronIT, advocaat], heeft toegang tot de data over heel Nederland. [zwartgelakt]
> op verzoek werden gegevens opgezocht en doorgespeeld. Dit werd erg gemakkelijk gemaakt doordat de medewerkers letterlijk iedereen konden opzoeken. […]
> HP Zone kent een query functie die het mogelijk maakt om bestanden eruit te trekken. Iedereen die toegang had kon ook hierbij. Er werd niet gemonitord wie wat deed. […]
> met behulp van de query functie zijn grote aantallen data aan het systeem [HPZone, advocaat] onttrokken en te koop aangeboden."

245. In een memo van 8 maart 2021 van GGD Haaglanden wordt nader ingegaan op het toekennen van rechten binnen HPZone (Lite) (**productie G.5**):

> "Binnen de applicatie zijn een tweetal rollen (Administrative-Officer en HPZoneNL Admin) waarmee gebruikers kunnen worden opgevoerd en rechten en autorisaties kunnen worden toegekend aan medewerkers die gebruik moeten maken van HPZone (Lite). De Administrative-Officer moet gekoppeld worden aan de HPZoneNL-Admin rol en vormt als zodanig een twee-eenheid. Gebruikelijk is dat dit soort rollen met verregaande rechtentoekenning, worden voorbehouden aan beheerders op het hoogste niveau die functioneel geautoriseerd zijn deze activiteiten uit te voeren. De situatie is echter nog iets complexer. Aan genoemde rollen zijn ook functionaliteiten ondergebracht die niet voorkomen in andere rollen maar wel noodzakelijk zijn voor een aantal medewerkers.
> Dit geldt ook voor het geven van meerdere accounts aan een landelijke BCO-medewerker. Hierdoor hebben landelijke BCO-medewerkers toegang tot de omgevingen van meerdere GGD'en, wat betekend [sic.] dat ze altijd in al deze omgevingen in kunnen loggen. Dit verhoogt de kans op onrechtmatige toegang en fraude, en verkleint die [sic.] kans op detectie van deze onrechtmatige toegang en fraude."

246. Geconcludeerd wordt dat een situatie is ontstaan waardoor meerdere medewerkers rollen hebben ontvangen waarmee zij hun werk kunnen uitvoeren maar daarnaast ook functionaliteiten kunnen gebruiken "*die kunnen leiden tot onrechtmatig handelen*". Blijkens een verslag van de GGD Haaglanden was deze situatie in april 2021 nog niet opgelost. Er bestonden op dat moment

nog steeds geen autorisatiematrixen omdat voor zowel CoronIT als HPZone de functionele beschrijvingen ontbraken (**productie G.52**).

247. Uit e-mailwisselingen van begin februari 2021 tussen GGD Drenthe en de Veiligheidsregio Drenthe blijkt dat naar aanleiding van de "dataperikelen" het toegangsproces tot HPZone is aangescherpt (**productie G.14**). Uit een notitie van 23 juni 2021 blijkt echter dat voor de corona-organisatie van GGD Flevoland "*het onterecht hebben van rechten*" nog steeds het hoogste risico is binnen het risicocluster "Gebruik (regio)" (**productie G.19**). Ook uit de DPIA Bron- en Contactonderzoek van GGD Rotterdam-Rijnmond blijkt dat (**productie G.27**):

> "Een aandachtspunt blijft dat de personen binnen HPZone nog steeds te open staat en dat iedereen nog te veel kan zien, zodra men binnen HPZone een rol heeft toegewezen".

248. Het gebrek aan (adequate) autorisatieprocedures heeft er ook daadwerkelijk toe geleid dat GGD-medewerkers toegang hadden tot veel meer gegevens dan zij nodig hadden.

249. In een groei- en voortgangsdocument van 25 juni 2021 van GGD Haaglanden wordt geconstateerd dat ten onrechte gebruikers van partnerorganisaties zijn geautoriseerd. Als gevolg daarvan is pas in februari 2021 een groot aantal gebruikers gedeactiveerd (**productie G.2** en **productie G.8**):

i. Rode Kruis: 03-02-2021 alle 703;
ii. VHD: 16-02-2021 alle 102;
iii. ANWB: 16-02-2021 alle 154;
iv. SOS international (@CED.nl en @SOSinternational.nl): totaal 1952 18-02-2021: medewerkers: 1095 gedeactiveerd
v. Eurocross: totaal 403 medewerkers

250. In het document wordt daarnaast geconstateerd dat binnen HPZone Lite rollen met de mogelijkheid tot het verstrekken van rechten aan medewerkers (intern of van partnerorganisaties) "direct" moeten worden beperkt (**productie G.2**).

251. Een ander intern document van GGD Haaglanden onderschrijft de gebrekkige maatregelen op het gebied van autorisaties (**productie G.10**):

> "Vanaf augustus 2020 is het aantal gebruikers dat rechten heeft om de CORONA map op de G: schijf in te zien en te wijzigen enorm toegenomen. Momenteel zijn er ongeveer 900 verschillende user accounts met volledige wijzigrechten op de gehele map CORONA. Het voordeel van deze situatie is dat een medewerker, zonder verdere tussenkomst van ICT, direct kan schakelen in verschillende rollen en werkzaamheden. Dit maakt de organisatie op dat gebied erg wendbaar. Er zijn echter ook erg veel nadelen en risico's, zoals:
> - geen zicht op wie waar rechten of toegang op heeft en zou moeten hebben
> - aanwezige data kan onaangekondigd gewijzigd, verplaatst of verwijderd worden
> - het doorvoeren van aanpassingen wordt bemoeilijkt door technische issues

- medewerkers kunnen hun werk baseren op verouderde instructies of gegevens

[…]

Uit navraag bij de verschillende teams binnen het Coronaprogramma blijkt dat meer dan 80% van het totaal aantal accounts geen wijzigrechten nodig heeft. Deze 80% willen we graag omzetten naar 'alleen-lezen' om de kans op een aantal van de eerder genoemde risico's te verminderen."

Niet of te laat aanpassen en intrekken van rechten

252. Ook bestond op de accounts die werden aangemaakt en vervolgens toegang hadden tot de systemen nauwelijks toezicht. Zo verklaarde een werknemer al "tientallen keren" een account aan te hebben laten aanmaken zonder enige controle (**productie C.8**). In een planbeschrijving van GGD Haaglanden die ziet op de veiligheid van de GGD-systemen wordt als risico van CoronIT en HPZone Lite geconstateerd dat er onvoldoende zicht bestaat op toegang tot en gebruik van gegevens. Erkend wordt dat dit risico kan leiden tot misbruik van gegevens door eigen of ingehuurde medewerkers (**productie G.9**).

253. Bovendien werden rechten niet of te laat aangepast of ingetrokken en zijn er tussen betrokken partijen onvoldoende afspraken gemaakt. Uit de stukken blijkt dat dit geen sporadische incidenten waren, maar dat sprake was van systematisch falen, mede veroorzaakt doordat er geen adequate procedures waren ingeregeld.

254. De risico's ten aanzien van het intrekken van autorisaties werden - voor zover Stichting ICAM kan nagaan: voor het eerst - geadresseerd in de BCO-DPIA van november 2020. Daaruit blijkt dat er een hoog risico bestond dat het vergeten van het intrekken van rechten van een BCO-medewerker, leidt tot onrechtmatige verwerking van persoonsgegevens (**productie G.15**):

"Applicatiebeheerders bij GGD'en moeten medewerkers van de landelijke schil rechten geven om in de systemen van de GGD te kunnen werken. Dit wordt vaak wel gedaan, maar door de drukte wordt vergeten de rechten in te trekken als de medewerker niet meer werkt voor die GGD. Daarnaast wordt vergeten de rechten op inactief te zetten als de medewerker bij een andere GGD wordt ingezet, waardoor de medewerker actieve inloggegevens heeft bij meerdere GGD'en, terwijl deze maar bij een GGD werkt op dat moment. Ook blijken medewerkers met gegevens van een andere GGD voor een GGD te werken. Hierdoor wordt het moeilijk na te gaan voor welke GGD is gewerkt en of de verwerkingen die de medewerker heeft uitgevoerd rechtmatig zijn, waardoor de kans op onder andere fraude toeneemt en fouten minder snel kunnen worden opgespoord.
Dit geldt ook voor het geven van meerdere accounts aan een landelijke BCO-medewerker. Hierdoor hebben landelijke BCO-medewerkers toegang tot de omgevingen van meerdere GGD'en, wat betekend [sic.] dat ze altijd in al deze omgevingen in kunnen loggen. Dit verhoogt de kans op onrechtmatige toegang en fraude, en verkleint die [sic.] kans op detectie van deze onrechtmatige toegang en fraude."

• De kans dat het risico zich manifesteert is hoog. De medewerkers kunnen gewoon bij de gegevens tot het account wordt verwijderd of op inactief wordt gezet. Dit in combinatie met slechte tot geen monitoring van de logging, zorgt ervoor dat niet kan worden achterhaald dat er iets fout gaat en de kans op fraude die door blijft gaan groot is.

> Met de multiples accounts kunnen medewerkers gelijktijdig toegang krijgen tot de verschillende omgeving waarbij deze medewerkers toegang krijgen tot een groot aantal persoonsgegevens.
> • De impact is hoog. Met de gegevens kan onrechtmatige inzage worden gegeven en fraude worden gepleegd. Hier kan de betrokkene grote gevolgen van ondervinden."

255. Al eerder uitten oud-GGD-medewerkers hun zorgen over het te laat intrekken van rechten. Zo kon een GGD-medewerker die wegens een gemiste training niet in dienst kon treden een maand later nog steeds in zijn account. In september 2020 vertelde hij RTV Oost: "*Je zou denken dat het account inmiddels geblokkeerd is. Ik heb vorige week eens geprobeerd in te loggen. En je raadt het al: dat lukte*" (**productie C.1**).

256. Door GGD Haaglanden wordt in een groei- en voortgangsdocument vastgesteld dat GGD-medewerkers daadwerkelijk niet of te laat werden afgemeld. Dit heeft ertoe geleid dat op 2 februari 2021 180 medewerkers van Randstad zijn gedeactiveerd en op 17 februari 2021 nog eens 194 GGD-medewerkers. Externe gebruikers van HPZone Lite werden bovendien ten onrechte ook opgevoerd in CoronIT en andersom. Verder wordt als risico genoemd dat het afnemen van autorisaties bij off-boarding niet technisch of organisatorisch is afgedwongen in HPZone Lite en CoronIT (**productie G.2**).

257. Dat het afmelden van externe gebruikers niet of te laat gebeurde, blijkt ook uit een interne e-mail van GGD Drenthe van 19 februari 2021 (**productie G.12**):

> "Ik heb vandaag een mogelijkheid in Hpzone ontdekt, die wij tot voor kort als niet mogelijk hebben geacht. Doormiddel van het combineren van 2 lijsten, is het mogelijk om alle gebruikers van webhelp die inactief zijn (in 2021 niet ingelogd) in beeld te krijgen. Ik schat dat het opschonen van deze lijst van 1723 externe gebruikers circa 8 uur zal kosten. Het sterke vermoeden bestaat dat daarmee het aantal gebruikers met toegang gehalveerd kan worden. Ik heb dit stuk met [zwartgelakt] besproken en die staat achter het houden van deze opschoonactie.
> Echter speelt er ook een nieuwe route vanuit landelijk (zie bijlage) die mogelijk op korte termijn definitief wordt. Bij ingaan van dit voorstel zal er een harde reset volgen waarbij alle externe gebruikers verwijderd zullen worden en daarna met nieuwe lijsten zullen de actieve gebruikers weer toegevoegd worden. De grote vraag is wanneer dit voorstel definitief wordt en wij deze harde reset kunnen gaan uitvoeren. Tot dat moment zitten de externe inactieve gebruikers nog in ons systeem."

258. Pas op 25 februari 2021 heeft GGD GHOR een procesvoorstel gedaan voor het opschonen van de autorisaties voor externe (landelijke) medewerkers in HPZone Lite, waarbij GGD'en bij ingang van het voorstel alle landelijke medewerkers moesten afmelden en daarna opnieuw actieve medewerkers moesten toevoegen (**productie G.13**). Uit het procesvoorstel blijkt bovendien dat niet iedere dag medewerkers bij de GGD aanwezig hoeven zijn met de juiste rechten om mensen aan en af te melden in HPZone Lite (**productie G.17**). Medewerkers die vanuit de flexibele landelijke capaciteit voor een GGD werken, worden niet doorlopend maar "op gezette tijden" afgemeld. In het Beleid Logische Toegangsbeveiliging van GGD IJsselland staat zelfs dat het uitgangspunt is dat controles van autorisaties slechts elke 6 maanden dienen te worden

uitgevoerd ten aanzien van informatiesystemen en applicaties waarin persoonlijke gezondheidsinformatie met de hoogste risico's is opgeslagen (**productie G.22**).

259. Dat de processen bij uitdiensttreding ook na het projectvoorstel van GGD GHOR nog niet goed waren ingeregeld, blijkt uit een intern document van de GGD Hollands-Noorden van 22 juni 2021. Bij uitdiensttreding wordt slechts per e-mail gevraagd of BCO-medewerkers alle data van de GGD hebben verwijderd. In dat document wordt bovendien als risico van het gebruik van eigen apparatuur benoemd dat medewerkers data lokaal downloaden waardoor bestanden "*rondslingeren*" met daarbij "*als direct gevolg het gevaar op een datalek of mogelijke handel in gegevens*" (**productie G.21**).

260. Ook na het datalek heeft de AP bij de onderzochte GGD'en geconstateerd dat medewerkers over autorisaties beschikten die zij voor hun werkzaamheden niet of niet langer nodig hadden. Het proces rond het tijdig aanpassen of intrekken van autorisaties verliep nog altijd niet goed. Duidelijke afspraken tussen de betrokken partijen zijn niet aangetroffen, ook niet naar aanleiding van het datalek (**productie K.1**).

Gebrek aan afspraken tussen betrokken partijen

261. De AP heeft tijdens haar onderzoek geconcludeerd dat duidelijke afspraken tussen de betrokken organisaties over bepaalde beveiligingsaspecten rondom de systemen die voor BCO worden gebruikt, ontbreken. Dit geldt bijvoorbeeld ten aanzien van het autorisatiebeheer en de controle van logbestanden. Hierdoor is onvoldoende duidelijk wie waarvoor verantwoordelijk is en wie welke maatregelen in dit verband dient te treffen. Dat vergroot de kans op nieuwe tekortkomingen in de beveiliging van persoonsgegevens. Daarnaast heeft GGD GHOR zelf aangegeven met de landelijke partners geen afspraken te hebben vastgelegd over het werken op eigen apparatuur. De AP concludeert met de opdracht aan GGD GHOR en de GGD'en om onderling en met de overige betrokken partijen per direct duidelijke afspraken op het vlak van informatiebeveiliging te maken, vast te leggen en actueel te houden. Voor partijen dient immers duidelijk te zijn wie voor welke technische en/of organisatorische maatregelen verantwoordelijk is. Dat was onvoldoende geregeld. Uit de gesprekken is namelijk het beeld naar voren gekomen dat met name ten aanzien van HPZone Lite onduidelijkheid bestaat over de verantwoordelijkheidsverdeling (**productie K.1**).

262. Voorgaande terwijl in de CoronIT-referentie-DPIA al is vastgesteld dat het gebrek aan afspraken tussen betrokken partijen een wezenlijk risico vormt voor de bescherming van de persoonlijke levenssfeer van betrokkenen (**productie G.1**):

> "6. Uitwisseling van gegevens met verschillende partijen kan leiden tot onrechtmatige uitwisseling van gegevens en gebrek aan overzicht van de uitwisselingen
> De gegevens uit CoronIT zijn voor verschillende partijen interessant of van belang. Daarom vinden verschillende uitwisselingen plaats en worden vragen gesteld om uitwisselingen te starten. Sommigen daarvan zijn in de wet bepaald, voor anderen wordt een grondslag gezocht. De snelle

ontwikkelingen en drukte kan leiden tot onzorgvuldige afweging van de uitwisseling, waardoor gegevens onrechtmatig kunnen worden uitgewisseld.

- De kans dat dit risico zich manifesteert is hoog. Over het algemeen worden de uitwisselingen op landelijk niveau aangevraagd, omdat dit voordelen oplevert. Binnen organisaties is vaak ook een lijn afgesproken om te beoordelen of de uitwisseling rechtmatig is. Er kunnen echter, door de drukte of door een medewerker die niet op de hoogte is dat een toetsing nodig is, gegevens worden uitgewisseld waar geen toetsing op is uitgevoerd.
- De impact van het risico is hoog. Vaak worden veel gegevens opgevraagd en daarbij ook de medische gegevens. Hier wordt vaak geen naam bij gegeven, maar sets kunnen naar personen worden herleid. Hoe meer informatie wordt gegeven, hoe sneller iemand kan worden herleid.

Geadviseerd wordt om de volgende maatregelen te treffen:

- Stel duidelijke richtlijnen op over de uitwisseling van data en neem daarin op dat eerst een toetsing moet plaatsvinden door iemand die daar in het kader van privacy een advies op kan geven.
- Wissel niet meer uit dan in het advies van de privacyspecialist is opgenomen. Het uitwisselen van (extra) gegevens kunnen namelijk leiden tot een ander advies.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

7. Wisselingen in partijen en verwerkingen kan leiden tot het niet maken van de juiste afspraken of onvoldoende grondslag

CoronIT is gemaakt om te ondersteunen in het bestrijden van de coronapandemie. Dit betekent dat de verspreiding sneller of trager kan gaan, waardoor veranderingen in het beleid, de verwerking en de partijen die meewerken ontstaan. Deze veranderingen kunnen snel gaan. Voor nieuwe partijen kan dit betekenen dat ze snel gaan meewerken, maar dat daardoor geen afspraken worden gemaakt over de verwerking van de persoonsgegevens. Wijzigingen in het beleid en/of de verwerking kunnen leiden dat snel gehandeld moet worden, waardoor een onjuiste of geen grondslag bestaat voor de verwerking.

- De kans dat het risico zich manifesteert is hoog. Continue verandering is vaak onder tijdsdruk, waardoor niet altijd kan worden nagedacht over de gevolgen van de veranderingen. Daarnaast is het snel aansluiten van partijen om het proces vlot te kunnen laten verlopen vaak belangrijk. Het opstellen van de juiste documenten en de onderhandeling daarover, vooral met betrekking tot privacy, kan daardoor worden vergeten.
- De impact van het risico is hoog. Onjuiste afspraken en geen of onvoldoende grondslag kan leiden tot onrechtmatige verwerking en/of het uitlekken van (medische) gegevens.

Geadviseerd wordt om de volgende maatregelen te treffen:

- Stel een duidelijke communicatielijn in over uitwisselingen en het aansluiten van nieuwe partijen, zodat kan worden of een grondslag bestaat of kan worden bekeken of, en zo ja welke, afspraken moeten worden gemaakt.

- Controleer periodiek of er wijzigingen zijn in partijen, de verwerking of nieuw beleid/nieuwe inzichten.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

10. Een overzicht van alle partijen, datastromen en uitwisselingen is niet opgesteld, waardoor gegevensstromen niet in kaart zijn, persoonsgegevens onrechtmatig worden verwerkt en uitlekken.

CoronIT is gelinkt met veel systemen. Daarnaast lopen nog processen langs CoronIT. Binnen GGD GHOR is geen totaaloverzicht van waar alle data wordt verwerkt en waar dat naar wordt uitgewisseld. Dit kan leiden tot het missen van stromen en onrechtmatige uitwisselingen, maar ook van het ontbreken van afspraken met partijen die de persoonsgegevens verwerken.

- De kans dat het risico zich voordoet is hoog. Er is geen totaal overzicht en daarom kan niet worden gezegd of alles is getoetst en of alles rechtmatig wordt uitgewisseld.
- Het impact van het risico is hoog. Gevoelige persoonsgegevens kunnen uitlekken, wat grote gevolgen heeft voor de betrokkene van wie de data is gelekt.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Breng de datastromen en afhankelijkheden rond de corona-applicaties in kaart.
- Toets na het in kaart brengen alle uitwisselingen en controleer of alle koppelingen zijn getoetst op beveiliging.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

263. Ten aanzien van het gebrek aan onderlinge afspraken wordt in de BCO-DPIA gewezen op het risico dat snelle ontwikkelingen vanwege de snelgroeiende vraag naar capaciteit, leiden tot verlies van overzicht en het niet (adequaat) maken van afspraken (**productie G.15**):

> "Binnen BCO is er een snelgroeiende vraag naar capaciteit, zodat GGD'en BCO adequaat kunnen uitvoeren. Deze vraag stijgt continu, waardoor nieuwe partijen, zowel verwerkers als subverwerkers, worden aangesloten. Hiervoor is geen centraal overzicht welke partijen exact meewerken en met wie wel en niet afspraken zijn gemaakt. Ook veranderd [sic] de werkwijze. Hierdoor kunnen verwerkersovereenkomsten achterlopen op de praktijk en dus niet de volledige verwerking bevatten. Dit betekent dat afspraken niet adequaat of volledig zijn gemaakt en dat persoonsgegevens onrechtmatig worden verwerkt, zowel in de wijze van verwerken, als de partij die deze persoonsgegevens verwerkt. […]"

264. Het gebrek aan afspraken, onder andere met betrekking tot de rolverdeling, tussen regionale en landelijke partners kan leiden tot onduidelijkheid in de verwerking van persoonsgegevens (**productie G.15**):

> "Voor het landelijke BCO traject heeft de intentie bestaan een convenant te sluiten tussen GGD GHOR en de GGD'en om duidelijke afspraken te maken over de taken van GGD GHOR en de GGD'en. De optie van het convenant is afgewezen, waardoor nu geen afspraken zijn gemaakt. Dit heeft een aantal nadelen. Zo is het niet duidelijk wie welke rollen heeft, maar bestaan er voor GGD GHOR ook problemen met de grondslag om contracten voor BCO te sluiten, omdat ze daar in eigen titel geen bevoegdheid en grondslag voor heeft."

265. Als gevolg van de inzet van verschillende callcenters, die elk eigen handelswijzen kennen, bestaat er een verhoogd risico op fraude, onrechtmatige verwerking en datalekken (**productie G.15**):

> "De inzet van verschillende callcentra bij verschillende GGD´en resulteert in verschillende methoden van aanmelding van landelijke BCO-werknemers volgens verschillende methodes. Dit kan leiden tot verwarring bij de aanvraag van autorisaties en daardoor kunnen mensen onrechtmatig toegang krijgen tot het systeem.
> Daarnaast werken callcentra vanuit hun eigen mailsystemen en met hun eigen telefoonnummers. Dit kan leiden tot verwarring bij betrokkenen, maar ook tot fraude. Mensen kunnen zich namelijk een e-mailadres aanmaken dat lijkt op het e-mailadres van het callcenter of bellen met een nummer en zich voordoen als een medewerker van het callcenter. Het is moeilijker te onderscheiden of het echt een landelijke BCO-medewerker is, of een fraudeur, omdat er geen centraal e-mailadres of telefoonnummer is.
> - De kans dat het risico zich manifesteert is midden. De GGD'en zijn op de hoogte van de contactgegevens van de landelijke partners. Daarnaast worden burgers steeds waakzamer op vreemde mails en verzoeken aan de telefoon.
> - De impact van het risico is hoog. Als een persoon onrechtmatige toegang krijgt, kan deze onrechtmatig gegevens verwerken. Dit geldt ook indien een persoon een vals nummer of emailadres aanmaakt. In dat geval kan er sprake zijn van fraude met de gegevens.
>
> Geadviseerd wordt om de volgende maatregelen te nemen:
> - Stel een uniforme werkwijze op zodat GGD'en weten dat de aanmelding van een landelijke BCO-medewerker echt door een landelijke partner wordt gedaan en stel een eenduidige werkwijze voor verificatie vast.
> - Communiceer de e-mailadressen en telefoonnummers van waaruit kan worden gebeld en zorg dat betrokkenen op de hoogte zijn wat deze mailadressen en telefoonnummers zijn. Stel betrokkenen ook op de hoogte van de vragen die ze mogen verwachten en wat zeker niet wordt gevraagd.

266. Uit voorgaande volgt dat de Staat c.s. onvoldoende maatregelen hebben getroffen op het gebied van autorisatie en daarmee in strijd gehandeld met artikel 5 lid 1 sub f en artikel 32 AVG.

4.2.4.4 Logging en monitoring

267. Het vastleggen van gebeurtenissen op IT-systemen in logbestanden en regelmatige controle daarvan vormt een belangrijk onderdeel van informatiebeveiliging. Aan de hand van de logbestanden kan worden nagegaan wie bepaalde gegevens heeft bekeken of aangepast. Ook kunnen uit logbestanden pogingen om ongeautoriseerd toegang te krijgen worden

geïdentificeerd. Ten aanzien van CoronIT en HPZone Lite is gebleken dat een deugdelijke en effectieve logging en controle ontbrak.

268. De NEN 7510 omschrijft welke beheers- en implementatiemaatregelen genomen moeten worden in het kader van logging en monitoring. Logbestanden die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren dienen te worden gemaakt, bewaard en regelmatig te worden beoordeeld. Logbestanden dienen het volgende te bevatten:[79]

a) Gebruikersidentificaties;

b) Systeemactiviteiten;

c) Data, tijdstippen en details van belangrijke gebeurtenissen, bijv. in en uitloggen;

d) Identiteit of indien mogelijk de locatie van de apparatuur en de systeemidentificatie;

e) Registratie van geslaagde en geweigerde pogingen om toegang te verkrijgen tot het systeem;

f) Registratie van goedgekeurde en geweigerde gegevens en overige pogingen om toegang te verkrijgen tot bronnen van informatie;

g) Systeemconfiguratieveranderingen;

h) Gebruik van speciale bevoegdheden;

i) Gebruik van systeemhulpmiddelen- en toepassingen;

j) Bestanden die zijn geopend en het type toegang dat is verkregen;

k) Netwerkadressen en –protocollen;

l) Alarmen die worden afgegeven door het toegangsbeveiligingssysteem;

m) Activering en deactivering van beschermingssystemen, zoals antivirussystemen en inbraakdetectiesystemen;

n) Verslaglegging van transacties die door gebruikers in toepassingen zijn uitgevoerd.

269. Verder dienen gezondheidsinformatiesystemen een beveiligd auditverslag (lees: een logbestand) aan te maken telkens wanneer een gebruiker toegang neemt tot gegevens of gegevens

[79] NEN 7510-2:2017, paragraaf 12.4.1, p. 89 e.v.

aanmaakt, bijwerkt of archiveert. Het auditverslag behoort op unieke wijze de gebruiker en de betrokkene te identificeren, de functie te identificeren die wordt uitgevoerd en het tijdstip en de datum te vermelden waarop de functie werd uitgevoerd. De faciliteit voor deze auditverslagen dient te allen tijde operationeel te zijn. Verder behoren berichtensystemen die worden gebruikt voor het overdragen van berichten met gegevens, een registratie bij te houden van die overdracht.[80] Ook schrijft de NEN 7510 uitgebreid voor dat en hoe logbestanden moeten worden beveiligd tegen vervalsing en onbevoegde toegang.[81]

270. Het belang van logging is gelegen in de bescherming van de persoonlijke levenssfeer. De NEN 7510 vermeldt daarover:

> "De eisen met betrekking tot het registreren en auditen behoren tot de belangrijkste van alle beveiligingseisen voor het beschermen van persoonlijke gezondheidsinformatie. Deze eisen garanderen rekenschap voor cliënten die hun informatie toevertrouwen aan elektronische registratiesystemen voor medische dossiers en zijn tevens een krachtige stimulans voor de gebruikers van dergelijke systemen om het beleid inzake het acceptabele gebruik van deze systemen na te leven. Doeltreffend auditen en registreren kan bijdragen aan het aantonen van misbruik van gezondheidsinformatiesystemen of van persoonlijke gezondheidsinformatie. Deze processen kunnen organisaties en cliënten ook helpen om schadeloosstelling te krijgen van gebruikers die hun toegangsrechten misbruiken. Eisen voor het registreren van gebeurtenissen worden in detail in NEN 7513 besproken."[82]

271. Specifiek voor logging bestaat dus een afzonderlijk NEN-norm, de NEN 7513. Daaruit volgt dat logging het in het algemeen mogelijk moet maken om achteraf onweerlegbaar vast te stellen welke gebeurtenissen hebben plaatsgevonden op een patiëntdossier.[83] Alle gebeurtenissen waarbij acties plaatsvinden die betrekking hebben op een patiëntdossier, moeten worden gelogd. Hiertoe behoren onder andere:[84]

a) Toegang tot dossiers;

b) Gegevens verwijderen, al dan niet op verzoek van de cliënt;

c) Gegevens lezen;

d) Gegevens kopiëren of afdrukken;

e) Overdragen van gegevens vanuit of naar een ander systeem of informatiedomein, met inbegrip van kopiëren op draagbare media;

[80] NEN 7510-2:2017, paragraaf 12.4.1, p. 90 e.v
[81] NEN 7510-2:2017, paragraaf 12.4.2, p. 91.
[82] NEN 7510-2:2017, paragraaf 12.4.1, p. 91.
[83] NEN 7513-2018, paragraaf 5.1, p. 15.
[84] NEN 7513-2018, paragraaf 6.1, p. 17-18.

f) Zoekacties.

272. Voor een betrouwbare logging moeten niet alleen de operationele gebeurtenissen in het gebruik van een informatiesysteem worden gelogd, maar ook de gebeurtenissen die van belang zijn voor de betekenis van de loggegevens en de gebeurtenissen die het loggen en de logging kunnen beïnvloeden, zoals de toegang tot de logging.[85] In- of uitschakelen van logging zelf dient altijd te worden gelogd.[86] Voorts behoort onder andere informatie te worden gelogd over toegangsregelingen[87] en over de toegang tot de logbestanden zelf.[88] Wijzigen of verwijderen van loggegevens behoort in beginsel niet voor te komen.[89]

273. Hoofdstuk 8 van de NEN 7513 bevat zekerheidseisen, zoals ten aanzien van de verantwoordelijkheid voor logging, de beschikbaarheid van logging en de bewaartermijn van loggegevens. Onder andere schrijft de NEN 7513 voor dat iedere zorginstelling zich dient te kunnen verantwoorden en daarom betrouwbare logging dient te hanteren. Daarom dient de zorginstelling een logbeheerder aan te wijzen.[90] Ook schrijft de NEN 7513 voor dat de logging zodanig beschikbaar moet zijn dat redelijkerwijze aan alle informatiebehoeften en wettelijke eisen kan worden voldaan. Daarbij wordt expliciet verwezen naar artikel 12 AVG.[91] Ten slotte dienen loggegevens, tenzij anders bepaald, minimaal 2 jaar en maximaal 15 jaar te worden bewaard.[92]

274. Ten aanzien van logging en monitoring is het uitgangspunt van de AP dat controle van de logging systematisch en consequent moet plaatsvinden. Een steekproefsgewijze controle en/of controle op basis van klachten is niet voldoende.[93] Bij willekeurig, steekproefsgewijs controleren is er volgens de AP geen sprake van een systematiek gericht op onrechtmatig gebruik en risico's. Zo heeft de AP geoordeeld dat met controle van de logging door aselecte steekproef van jaarlijks zes patiëntdossiers, het HagaZiekenhuis geen beleid had ten aanzien van systematische, risicogerichte c.q. intelligente controle van de logging.[94] Ook in de praktijk had volgens de AP geen systematische controle van de logging plaatsgevonden, want de controles die wel hadden plaatsgevonden waren naar aanleiding van enkele klachten en verzoeken maar niet risicogericht en waren in omvang onvoldoende, gelet op de schaal van de verwerking van het ziekenhuis. Dat betekende volgens de AP dat het HagaZiekenhuis niet voldeed aan norm 12.4.1 van de NEN 7510. Daarmee was geen sprake van passende maatregelen ten aanzien van controle van de logging

85 NEN 7513-2018, paragraaf 6.1, p. 17.
86 NEN 7513-2018, paragraaf 6.4.1, p. 19.
87 NEN 7513-2018, paragraaf 6.3.2, p. 19.
88 NEN 7513-2018, paragraaf 6.4.2, p. 19.
89 NEN 7513-2018, paragraaf 6.4.3, p. 19.
90 NEN 7513-2018, paragraaf 8.2, p. 38.
91 NEN 7513-2018, paragraaf 8.3, p. 38.
92 NEN 7513-2018, paragraaf 8.5, p. 40.
93 AP, 'Toegang tot digitale patiëntdossiers door medewerkers van het HagaZiekenhuis', 26 maart 2019, p. 13.
94 AP, 'Toegang tot digitale patiëntdossiers door medewerkers van het HagaZiekenhuis', 26 maart 2019, p. 14.

zoals vereist ingevolge artikel 32 lid 1 AVG. De AP legde een boete op van € 460.000,- (waarbij ook meewoog dat het HagaZiekenhuis geen tweefactor-authenticatie had ingevoerd).[95]

275. Ook was volgens de AP in een zaak tegen het OLVG-ziekenhuis het doen van slechts acht incidentele controles en twee proactieve steekproeven in een periode van 15,5 maanden ruimschoots en evident onvoldoende om te kunnen spreken van een passend beveiligingsniveau dat ziet op het signaleren van onbevoegde toegang tot patiëntgegevens en het treffen van maatregelen naar aanleiding van onbevoegde toegang. Daarbij achtte de AP van belang de schaal van de verwerking van gezondheidsgegevens door het ziekenhuis, de gevoelige aard van de gegevens en de risico's voor de persoonlijke levenssfeer van betrokkenen. De AP legde een boete op van € 440.000,- (waarbij ook meewoog dat het OLVG-ziekenhuis geen tweefactor-authenticatie had ingevoerd).[96]

276. Volgens GGD GHOR is bij de bouw van HPZone en CoronIT bewust de keuze gemaakt om wel te loggen, maar om niet automatisch en continu logs te monitoren.[97] In plaats van automatische controles, heeft slechts steekproefsgewijze controle van de logging plaatsgevonden.[98] Medewerkers van de GGD'en bevestigen dat het om niet-automatische, willekeurige checks ging. Het aantal steekproeven is pas na de uitzending van Nieuwsuur opgeschroefd (paragraaf 3.1.1).[99]

277. In september 2020 heeft GGD GHOR, in antwoord op vragen van de AP naar aanleiding van een eerdere datalekmelding, aangegeven dat in het vierde kwartaal van 2020 geautomatiseerde controle van de logbestanden zou worden ingericht. Op basis van deze informatie besloot de AP destijds de datalekmelding af te sluiten. In januari 2021 bleek deze geautomatiseerde controle nog niet te zijn ingericht. Na de berichtgeving door RTL Nieuws van januari 2021 gaf GGD GHOR aan de geautomatiseerde controle in de vorm van een SIEM-oplossing (Security Information & Event Management) versneld te zullen implementeren. Deze zou eind maart 2021 gereed zijn. Ook deze planning is niet gehaald. De AP constateert dat de SIEM-oplossing in ieder geval ten tijde van het afronden van de onderzoeksfase in juni 2021 nog steeds niet was geïmplementeerd (**productie K.1**).

278. Door GGD GHOR zou zijn aangegeven dat toegang en zoekopdrachten werden gelogd.[100] Voor een groot aantal handelingen zou volgens GGD GHOR achterhaald moeten kunnen worden welke persoon deze heeft uitgevoerd.[101]

---

95 AP, 'Besluit tot het opleggen van een bestuurlijke boete en een last onder dwangsom HagaZiekenhuis', 18 juni 20219. De boete is door de rechtbank Den Haag verlaagd tot € 350.000,- omdat het HagaZiekenhuis wel enkele andere maatregelen had getroffen: Rechtbank Den Haag 31 maart 2021, ECLI:NL:RBDHA:2021:3090 (*AP/HagaZiekenhuis*).
96 AP, 'Besluit tot het opleggen van een bestuurlijke boete OLVG', 26 november 2020, p. 12.
97 *Kamerstukken II* 2020/21, 27 529, nr. 234, p. 19 (**productie D.2**).
98 *Kamerstukken II* 2020/21, 27 529, nr. 234, p. 19 (**productie D.2**).
99 *Kamerstukken II* 2020/21, 27 529, nr. 234, p. 24 (**productie D.2**).
100 *Kamerstukken II* 2020/21, 27 529, nr. 234, p. 25 (**productie D.2**).
101 *Kamerstukken II* 2020/21, 27 529, nr. 234, p. 4 (**productie D.2**).

279. De AP heeft in haar onderzoek naar aanleiding van het GGD-datalek ten aanzien van twee GGD'en geconcludeerd dat er wel logbestanden werden gemaakt van gebeurtenissen die in de systemen plaatsvonden, 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. Naar aanleiding van het datalek en in afwachting van een SIEM-oplossing, zou GGD GHOR dagelijkse handmatige controle van de logbestanden van CoronIT en HPZone (Lite) hebben ingericht (**productie K.1**).

280. Hoewel de AP ervan uit lijkt te gaan dat door de Staat c.s. wel logbestanden zijn aangemaakt, is onzeker of dit voor alle GGD'en gold en is geheel onduidelijk van welke gebeurtenissen op de IT-systemen nu wel en niet logbestanden zijn bijgehouden. Ook zijn noch de Staat noch GGD GHOR noch de GGD'en tot op heden in staat geweest sluitend vast te stellen van hoeveel mensen gegevens onbevoegd zijn ingezien en/of ontvreemd, zoals door middel van ongeoorloofde exports (zie paragraaf 3.1.10 en 3.4). Als al logging heeft plaatsgevonden, dan is deze dus zeer gebrekkig geweest en is er geen sprake geweest van (adequate) controle van logging.

281. Volgens de CoronIT-referentie-DPIA zouden op CoronIT twee soorten logging worden bijgehouden (**productie G.1**):

> "Functionele logging (of audit trail).
> In deze logging is te zien wat in het dossier is gebeurt [sic]. Dit betekent dat kan worden gezien welke delen van het dossier zijn geopend, door wie en wanneer. Daarnaast is te zien of er wijzingen of andere bewerkingen zijn geweest in de gegevens.
> Deze logging kan door GGD GHOR Nederland zelf worden ingezien. Ook het inzien van de logging wordt daarbij gelogd.
> Op deze logging worden geen signalen gegeven bij afwijkingen. Er zijn hiervoor geen afwijken [sic.] gedefinieerd.
> De functionele logging wordt nooit verwijderd.
> Technische logging
> De techinsche [sic.] logging geeft weer wat de applicatie wegschrijft. In principe worden hier geen persoonsgegevens in opgeslagen. Bij uitzondering kunnen echter wel zaken als een IP-adres worden opgeslagen.
> De technische logging is bij Topicus op te vragen indien GGD GHOR Nederland deze in wil zien.
> Op de technische logging is signalering ingericht, die in werking treedt als een drempelwaarde wordt bereikt.
> Op de logging wordt logging toegepast. Deze wordt beveiligd middels keyhub."

282. In de CoronIT-referentie-DPIA wordt echter als hoog risico aangemerkt het gebrek aan logging van het afsprakenoverzicht en de controle op logging in het algemeen (**productie G.1**):

> "1. Geen logging van inzage afsprakenoverzicht

Binnen CoronIT is geen logging aangezet op de inzage van het afsprakenoverzicht. In het afsprakenoverzicht is de naam, geboortedatum, geslacht, testlocatie, testdatum en testtijd te zien. Medewerkers kunnen zich hierdoor onrechtmatig inzage verschaffen in afspraakgegevens van betrokkenen.

- De kans dat dit risico zich manifesteert zonder maatregelen is hoog. Immers is het afsprakenoverzicht voor medewerkers toegankelijk en bijvoorbeeld snel worden gecontroleerd wanneer de afspraak van iemand is gepland.
- De impact van dit risico zonder maatregelen is middel. De gegevens bevatten geen medische gegevens, maar wel waar iemand op een exact moment te vinden is.

Geadviseerd wordt om de volgende maatregelen te nemen:

- Activeer logging op het afsprakenoverzicht, zodat duidelijk is wie zich wanneer toegang heeft verschaft tot het afsprakenoverzicht.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Laag

2. Geen controle op de logging

Binnen CoronIT is logging ingeregeld, maar de logging wordt niet actief op periodieke wijze en automatisch gecontroleerd. Voor deze controle is geen beleid opgezet, zodat niet is vastgelegd hoe en door wie deze controle zal worden uitgevoerd. Hierdoor is de kans groot dat misbruik wordt gemaakt van de gegevens in CoronIT, maar dat dit niet wordt opgemerkt.

- De kans dat het risico zich manifesteert zonder maatregelen is hoog. Er zijn veel autorisaties uitgegeven voor toegang tot CoronIT, waarbij medewerkers en externen toegang hebben tot (een bepaald deel van) de gegevens. Bij de aantallen medewerkers die in dienst zijn en zijn ingehuurd, is de kans groot dat iemand, kwaadwillend of niet, onrechtmatig dossiers opent.
- De impact van het risico is hoog. In CoronIT zijn medische gegevens en het BSN opgenomen, alsook contactgegevens. Hier kan op verschillende wijze misbruik van worden gemaakt.

Geadviseerd worden om de volgende maatregelen te nemen:

- Stem met de GGD'en af wie verantwoordelijk is voor welke deel van de controle van de logging. Dit kan worden opgenomen in het convenant/een addendum bij het convenant.
- Stel een beleid/procedure op voor de controle van de logging, dat voldoet aan de toepasselijke norm, de NEN 7513.
- Implementeer het beleid/de procedure in de organisatie en controleer zo snel mogelijk de logging. Indien dit niet met software kan, stel dan medewerkers aan die dit controleren tot de software wel beschikbaar is. Als met software wordt gecontroleerd, moet alsnog een menselijke controle worden uitgevoerd op een steekproef van de door de software gecontroleerde logbestanden.
- Zorg voor een sanctiebeleid waarin is opgenomen wat met de medewerker gebeurt indien hij niet werkt volgens de gestelde regels en zorg dat de medewerkers hiervan op de hoogte zijn.

Risico voor Betrokkene (voor maatregelen)	Hoog
Risico voor Betrokkene (na maatregelen)	Middel

Het restrisico na genomen maatregelen is dat de controle van logging niet iedere medewerker en iedere inzage van het dossier kan controleren. Hierdoor blijft een risico bestaan dat medewerkers toch onrechtmatig dossiers inzien en de gegevens misbruiken. De medewerkers werken in een groot deel van de gevallen thuis, waardoor ook geen onderling toezicht op de werkvloer bestaat."

283. Als beveiligingsmaatregel wordt in het kader van logging en monitoring aangegeven dat controle ad hoc plaatsvindt, na een vermoed of vastgesteld incident. Voor de controle van logging is geen procedure opgesteld, maar zouden wel plannen zijn opgesteld voor hoe logging dient te worden gecontroleerd voor ten minste medewerkers van het callcenter (**productie E.1**).

284. Uit de BCO-DPIA blijkt dat als hoog risico is aangemerkt dat onvoldoende logging en controle op en monitoring van logging leidt tot het niet opsporen van onrechtmatige verwerkingen (**productie G.15**):

> "Voor de uitvoering van de werkzaamheden van de medewerkers is het noodzakelijk dat wordt gelogd wat de medewerkers in de dossiers doen. Dit betekent dat gecontroleerd wordt of de handelingen die zei [sic.] uitvoeren met betrekking tot de persoonsgegevens rechtmatig zijn. Dit kan door controle van de logging. Indien deze controle niet wordt uitgevoerd, kunnen onrechtmatige verwerkingen niet worden opgespoord en afgehandeld.
> - De kans dat het risico zich manifesteert is hoog. Medewerkers worden ingezet bij GGD'en, die zelf moeten monitoren. Het is niet bekend of deze logging bij iedere GGD wordt gecontroleerd en of wordt gekeken naar de BCO-medewerkers van de landelijke schil die worden ingezet.
> - De impact van het datalek is hoog. Het aantal gegevens waar toegang toe wordt gekregen, bevatten gegevens die gevoelig zijn, zoals medische gegevens, maar ook gegevens die extra beschermd worden, zoals een BSN. Het uitlekken van deze persoonsgegevens kan grote gevolgen hebben, zoals fraude met deze persoonsgegevens.
>
> Geadviseerd wordt om de volgende maatregelen te nemen:
>
> - Zorg dat met iedere verwerker en met de GGD'en wordt afgesproken dat de is [sic.] logging ingeschakeld en periodiek wordt gecontroleerd. Controle van de logging is een verantwoordelijkheid van de GGD'en. Voor de controle is een procedure nodig, waarbij rekening wordt gehouden met de omstandigheden waaronder wordt ±gewerkt [sic.], het aantal mensen dat werkt en het aantal persoonsgegevens dat wordt verwerkt.
> - Zorg voor een uniforme werkwijze bij het opsporen van onrechtmatige activiteiten en indien opzettelijk, de sancties die worden gegeven.
>
> Het restrisico is dat door de grote aantallen medewerkers, die constant wisselen en die thuis werken, de kans op fraude en onrechtmatig gebruik blijft bestaan. Er is geen controle op de werkvloer en met periodieke controle kan niet alles worden gecontroleerd. Zo kan iemand gemakkelijk niet worden opgemerkt."

285. Uit een e-mailwisseling van de gemeente Rotterdam blijkt dat er op HPZone in het geheel niet werd gemonitord op gebruik van de query-functie. In deze e-mail wordt vermeld dat "*HP Zone een query functie [kent] die het mogelijk maakt om bestanden eruit te trekken. Iedereen die toegang had kon ook hierbij. Er werd niet gemonitord wie wat deed. […] met behulp van de query functie zijn grote aantallen data aan het systeem [HPZone, adv.] onttrokken en te koop aangeboden*." Ook wordt opgemerkt dat "*HP Zone de query functie wel [logt] en het niet moeilijk te zien [is] wie welke query heeft gedraaid*", maar dat deze functie "*niet pro actief [is] gebruikt*" (**productie G.41**). In de context van de betreffende e-mail, betekent deze laatste opmerking dat

de logging van de query functie niet heeft plaatsgevonden. Dat volgt ook uit het vervolg van de e-mail:

> "Grote groepen nieuwe BCO medewerkers die snel werden opgeleid kregen toegang [tot HPZone Lite, adv.] en werken meestal vanuit huis. Kwaadwillende medewerkers konden gegevens nazien over de regio's' tot welke ze toegang kregen. Ze konden allemaal de query functie gebruiken om gegevens over te halen naar Excel. De medewerkers moesten een VOG overleggen bij aantreden en een geheimhoudingsverklaring tekenen. Daarna zijn hun acties op het systeem zijn [sic] niet gevolgd of gecontroleerd.[…]"

286. Ook in het groei- en voortgangsdocument van 25 juni 2021 van GGD Haaglanden wordt ten aanzien van HPZone (Lite) en CoronIT vastgesteld dat controle op onterechte inzage pas achteraf via logging wordt geconstateerd en "die vangt maar heel weinig af"(**productie G.2**).

287. Uit een notitie van de GGD Noord- en Oost Gelderland d.d. 23 juli 2021 blijkt dat op die datum de "controle op de logging nog onvoldoende plaatsvond" en dat er "nog geen goed uitgewerkte regeling was voor monitoring en logging van gebruikershandelingen" (**productie G.43**).

288. Gezien de gevoelige aard van de gegevens, de grote omvang van de verwerking en de risico's voor de persoonlijke levenssfeer van Betrokkenen hadden de Staat c.s. veel ruimer gebruikershandelingen moeten loggen, waaronder in ieder geval het gebruik van export- en printfunctionaliteiten, en de loggegevens systematisch, risicogericht en consequent moeten controleren. Dit is een van de belangrijkste beveiligingseisen voor het beschermen van gezondheidsgegevens.[102] Op deze manier had onbevoegde toegang kunnen worden gesignaleerd en hadden maatregelen kunnen worden genomen. Gelet op de schaal van verwerkingen door de GGD'en, had de controle ook in omvang substantieel moeten zijn. De Staat c.s. hebben niet voldaan aan het vereiste van het systematisch, risicogericht en consequent beoordelen van logbestanden, wat in de context van deze verwerking in het kader van artikel 32 van de AVG wel is vereist.

289. Uit voorgaande volgt dat de Staat c.s. geen passend beschermingsniveau heeft geboden, in strijd met artikel 5 lid 1 sub f AVG en artikel 32 AVG.

4.2.4.5 Screening en toezicht

290. Bij het verwerken van persoonsgegevens, en in het bijzonder wanneer het gaat om grote hoeveelheden gevoelige en bijzondere persoonsgegevens, is het van groot belang dat het personeel dat toegang heeft tot de gegevens, gekwalificeerd en betrouwbaar is. Onderdeel van een passend niveau van beveiliging is dan ook dat medewerkers (zowel eigen medewerkers als medewerkers van contractanten) die toegang hebben tot gegevens, worden gescreend, dat

[102] Zie ook: Rb. Zeeland-West-Brabant, 21 september 2022, ECLI:NL:RBZWB:2022:5457 (*X/Bravis Ziekenhuis*), r.o. 4.31.

wordt beoordeeld in hoeverre zij geschikt zijn voor de werkzaamheden en dat wordt gewaarborgd dat zij hun verantwoordelijkheden begrijpen. Ten aanzien van de tienduizenden GGD-medewerkers die toegang hadden tot de GGD-systemen is gebleken dat screening en toezicht onvoldoende waren.

291. De NEN 7510 omschrijft de volgende beheersmaatregelen die in acht moeten worden genomen ten aanzien van screening en controle:

a) Ten eerste behoort de achtergrond van alle kandidaten te worden geverifieerd voorafgaand aan het dienstverband, op een wijze in verhouding tot de bedrijfseisen, de classificatie van de gegevens waartoe toegang wordt verleend en de vastgestelde risico's. Minimaal dienen de identiteit, het huidige adres en de vorige werkkring te worden geverifieerd. Indien wettelijk toegestaan, dient verificatie ook een controle op een strafblad te omvatten. Ten aanzien van contractanten geldt dat de overeenkomsten de verantwoordelijkheden voor het uitvoeren van de screening dienen te vermelden en de procedure die gevolgd moet worden als de screening niet is afgemaakt of als de resultaten aanleiding geven tot twijfel of bezorgdheid;[103]

b) Ten tweede behoort de contractuele overeenkomst met medewerkers en contracten hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden. Beveiligingsrollen en –verantwoordelijkheden, zoals vastgelegd in het informatiebeveiligingsbeleid van de organisatie, behoren ook in relevante functieomschrijvingen te worden vastgelegd. Speciale aandacht behoort te worden besteed aan de rollen en verantwoordelijkheden van tijdelijk personeel of personeel met een kort dienstverband. Onder andere dienen alle medewerkers en contractanten een vertrouwelijkheids- of geheimhoudingsovereenkomst te ondertekenen voordat hen toegang wordt verleend tot gegevens en dient hun contract te vermelden welke actie moet worden ondernomen als de medewerkers of contractanten de beveiligingseisen veronachtzamen. Waar van toepassing behoren de verantwoordelijkheden voor een vastgestelde periode na het einde van het dienstverband van kracht te blijven;104

c) Ten derde behoort de directie tijdens het dienstverband van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie. Zij dienen op de juiste wijze te worden geïnstrueerd voordat zij toegang krijgen tot gegevens, dienen richtlijnen te ontvangen die de verwachtingen met betrekking tot hun informatiebeveiligingsrol aangeven en dienen continu te beschikken over de juiste vaardigheden en kwalificaties. Alle medewerkers en contractanten dienen een passende en periodieke

[103] NEN 7510-2:2017, paragraaf 7.1.1, p. 24 e.v.
[104] NEN 7510-2:2017, paragraaf 7.1.2, p. 26 e.v.

bewustzijnsopleiding en –training te krijgen en regelmatige bijscholing, welke regelmatig dienen te worden geüpdatet;[105]

d) Ten vierde behoort er een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die inbreuk maken op de informatiebeveiliging;[106]

e) Ten vijfde behoren verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, te worden gedefinieerd, gecommuniceerd en ten uitvoer gebracht.[107]

292. Volgens GGD GHOR moesten medewerkers van de GGD'en en van externe partijen een VOG aanleveren en een geheimhoudingsverklaring ondertekenen.[108] Volgens GGD GHOR wordt een VOG verstrekt op basis van een toetsing op het profiel dat voor de betreffende functie is vastgesteld, waardoor het zo kan zijn dat een medewerker veroordeeld is voor strafbare feiten die niet relevant zijn voor de functie waarvoor de VOG is aangevraagd.[109]

293. Gebleken is echter dat deze maatregelen ten behoeve van screening en toezicht van medewerkers in werkelijkheid niet (volledig en juist) geïmplementeerd zijn. De screening van medewerkers was in veel gevallen nog niet afgerond op het moment dat de betreffende medewerker aan het werk ging. Sommige medewerkers hebben zelfs helemaal geen VOG aangeleverd. Een aantal medewerkers kreeg pas toen het datalek aan het licht kwam het verzoek een VOG aan te leveren (**productie C.3**). Er hebben zich dus situaties voorgedaan waarin medewerkers wel toegang hadden tot systemen, terwijl zij geen VOG hadden overlegd,[110] en terwijl deze VOG volgens GGD GHOR juist werd gebruikt als screeningsmiddel.[111] Het exacte aantal is volgens GGD GHOR niet bekend gezien de aantallen en de verschillende arbeidsrelaties.[112] Ook heeft GGD GHOR bevestigd dat elk van de ingeschakelde derden zijn eigen controlesystematiek hanteert, hetgeen erop duidt dat een eenduidig beleid dus ontbrak.

294. Zo blijkt uit een mailwisseling van GGD Hart voor Brabant van maandag 8 februari 2021, getiteld "*RE: SPOED: Gemeenteraadsvragen over AVG"* dat medewerkers toegang hadden tot de systemen ondanks dat zij geen VOG hadden. Pas na het bekend worden van het GGD-datalek heeft GGD Hart voor Brabant acties uitgezet om te controleren of dit wel had moeten gebeuren.

---

105 NEN 7510-2:2017, paragraaf 7.2.1 en 7.2.2, p. 27 e.v.
106 NEN 7510-2:2017, paragraaf 7.2.3, p. 30 e.v.
107 NEN 7510-2:2017, paragraaf 7.3.1, p. 31 e.v.
108 *Kamerstukken II* 2020/21, 27 529, nr. 234, p. 3 (**productie D.2**).
109 *Kamerstukken II* 2020/21, 27 529, nr. 234, p. 3 (**productie D.2**).
110 *Kamerstukken II* 2020/21, 27 529, nr. 234, p. 3 (**productie D3**).
111 *Kamerstukken II* 2020/21, 27 529, nr. 234, p. 52 (**productie D.2**).
112 *Kamerstukken II* 2020/21, 27 529, nr. 234, p. 3 (**productie D.2**).

295. Uit een oplegnotitie van de GGD Rotterdam-Rijnmond blijkt dat daar het proces zo was ingericht dat de circa 1.600 medewerkers die toegang hadden tot HPZone en CoronIT, reeds aan het werk gingen en toegang kregen tot persoonsgegevens op het moment dat hun VOG nog werd aangevraagd, terwijl op dat moment dus nog niet zeker was dat die aanvraag zou worden goedgekeurd. Dat heeft ertoe geleid dat op de datum van die notitie, 9 februari 2021, meer dan 400 medewerkers werkzaam waren en toegang hadden tot bijzondere persoonsgegevens van miljoenen mensen zonder dat er een VOG was aangevraagd, althans goedgekeurd (**productie G.37**, p. 5).

296. Zoals uiteengezet bestond ook nauwelijks toezicht op en controle van medewerkers. Zo bestond op de accounts die werden aangemaakt en die vervolgens toegang hadden tot de systemen nauwelijks toezicht en konden werknemers accounts aan aanmaken zonder enige controle (**productie C.8**). Ook konden medewerkers op verzoek gegevens van bekende personen en bekende Nederlanders opzoeken in de systemen (**productie C.4**). In de CoronIT-referentie-DPIA wordt in dat kader als restrisico erkend dat medewerkers in een groot deel van de gevallen thuiswerken, waardoor geen onderling toezicht bestaat (**productie G.1**).

297. Dat er nauwelijks serieuze controles plaatsvonden is, zoals aangegeven, ook door medewerkers verklaard "*Enkele werknemers vertellen hoe ze eens in de zoveel maanden hun scherm via Microsoft Teams moeten delen om vervolgens de digitale prullenbak te openen. De manager kijkt dan of daar gestolen gegevens uit de coronasystemen in te vinden waren. "'Een wassen neus', wordt het genoemd.*" (**productie C.8**).

298. Medewerkers zouden volgens GGD GHOR interne trainingen moeten volgen. De training van de landelijke partners is hetzelfde, per GGD kan echter de training verschillen. Dit betekent dat niet alle medewerkers (dezelfde) training hebben gehad omtrent privacy en gegevensbescherming. Daarbij kwam in februari 2022 aan het licht dat tijdens een training van nieuwe medewerkers in december 2021 klassikaal persoonsgegevens werden getoond van iemand die een vaccinatieafspraak had gemaakt (**productie C.17**). Ten aanzien van de kwaliteit van deze trainingen kunnen dan ook twijfels worden geuit.

299. Uit een Projectplan Awareness Campagne Informatiebeveiliging 2021 van de GGD Noord- en Oost-Gelderland d.d. 15 februari 2021 blijkt dat het op dat moment nog slechts een doelstelling was ervoor te zorgen dat "voor 1 januari 2022 90% van de medewerkers de (nieuwe) geheimhoudingsverklaring zou hebben ondertekend" en "voor 1 juni 2022 75% van de medewerkers een E-learning zou hebben gevolgd" (**productie G.46**, p. 12).

300. Uit voorgaande volgt dat de Staat c.s. geen passend beschermingsniveau heeft geboden, in strijd met artikel 5 lid 1 sub f AVG en artikel 32 AVG.

4.2.5 Schending van het beginsel van dataminimalisatie (artikel 5 lid 1 sub c AVG)

301. Uitsluitend persoonsgegevens die toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor het doeleinde, mogen worden verwerkt. Dit brengt volgens de EDPB mee dat de verwerkingsverantwoordelijke vooraf moet bepalen welke kenmerken en parameters van verwerkingssystemen en hun ondersteunende functies toelaatbaar zijn.[113] Het beginsel van dataminimalisatie geldt niet alleen voor de hoeveelheid verzamelde persoonsgegevens, maar ook voor de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan.[114] De AVG eist in dat verband dat passende technische en organisatorische maatregelen worden getroffen om de inachtneming van het beginsel van gegevensminimalisatie te garanderen.

302. Tienduizenden (deels extern ingehuurde) GGD-medewerkers hadden echter op grote schaal toegang tot CoronIT en HPZone (Lite) en daarmee tot een grote hoeveelheid (bijzondere) persoonsgegevens waarover zij niet hoefden te beschikken. Zij hadden bovendien de mogelijkheid deze gegevens te doorzoeken, te printen en te exporteren. De Staat c.s. hadden op basis van een beoordeling van de noodzaak moeten beperken wie er toegang hadden tot persoonsgegevens en welke soorten toegang er werden verleend. Dat is niet gebeurd, zelfs niet nadat hen dat door de AP werd opgedragen.

303. Ook werden in de GGD-systemen meer persoonsgegevens verwerkt dan strikt noodzakelijk was. Zo blijkt uit een memo van de MT Corona Crisis organisatie van de gemeente Rotterdam dat na het bekend worden van het GGD-datalek, besloten is om bepaalde persoonsgegevens voortaan niet langer op te slaan, althans niet langer toegankelijk te maken voor alle medewerkers. Dat betekent dat deze verwerkingen dus in de eerste plaats al niet noodzakelijk waren. Uit het memo blijkt onder andere dat het niet nodig was om BSN's te verwerken in HPZone Lite, aangezien ook had kunnen worden volstaan met een combinatie van naam/geboortedatum en postcode (**productie G.42**).

304. Door een gebrek aan toegangscontrole, autorisaties en autorisatiebeheer, en door meer gegevens te verwerken dan noodzakelijk, hebben de Staat c.s. het beginsel van minimale gegevensverwerking niet kunnen waarborgen en hebben de Staat c.s. niet voldaan aan het beginsel van dataminimalisatie zoals neergelegd in artikel 5 lid 1 onderdeel c AVG.

---

113 EDPB, 'Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaardinstellingen', versie 2.0, vastgesteld op 20 oktober 2020, p. 24.

114 Artikel 25(2) AVG. EDPB, 'Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaardinstellingen', versie 2.0, vastgesteld op 20 oktober 2020, p. 14.

4.2.6 Schending van het beginsel van gegevensbescherming door ontwerp en door standaardinstellingen (artikel 25 AVG)

305. *Privacy-by-design* en *privacy-by-default* zijn twee verplichte uitgangspunten in artikel 25 AVG.[115] Bij privacy-by-design gaat het om aandacht voor gegevensbescherming in de ontwerpfase van een product of dienst. Privacy-by-default houdt in dat standaardinstellingen zo privacy-vriendelijk mogelijk moeten zijn. Deze verplichtingen gelden gedurende de gehele verwerkingscyclus en ook uitdrukkelijk voor verwerkingssystemen die al bestonden voordat de AVG in werking trad.[116]

306. Overeenkomstig artikel 25 lid 1 AVG moet de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen treffen die zijn ontworpen om de gegevensbeschermingsbeginselen (artikel 5 AVG) op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking inbouwen ter naleving van de voorschriften en ter bescherming van de rechten van de betrokkenen (gegevensbescherming door ontwerp; *privacy-by-design*). Passend houdt in dat de maatregelen en noodzakelijke waarborgen geschikt moeten zijn voor het beoogde doel, oftewel dat hiermee de gegevensbeschermingsbeginselen op een doeltreffende manier worden uitgevoerd.[117]

307. Ingevolge artikel 25 lid 2 AVG, treft de verwerkingsverantwoordelijke daarnaast passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking (gegevensbescherming door standaardinstellingen; *privacy-by-default*). Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. De verwerkingsverantwoordelijke moet op basis van een beoordeling van de noodzaak beperken wie er toegang hebben tot persoonsgegevens en welke soorten toegang er worden verleend. Toegangscontroles moeten tijdens de verwerking worden geëerbiedigd voor de hele gegevensstroom.[118]

308. Een “standaardinstelling” verwijst volgens de EDPB naar de reeds bestaande of vooraf geselecteerde waarde van een configureerbare instelling die is toegekend aan een applicatie, computerprogramma of apparaat (“voorinstellingen” of “fabrieksinstellingen”). Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke om dusdanige standaardinstellingen

[115] De beginselen worden beschreven in artikel 5 en overweging 39 van de AVG.
[116] EDPB, ‘Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaardinstellingen’, versie 2.0, vastgesteld op 20 oktober 2020, p. 5.
[117] EDPB, ‘Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaard-instellingen’, versie 2.0, vastgesteld op 20 oktober 2020, p. 6-7.
[118] EDPB, ‘Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaard-instellingen’, versie 2.0, vastgesteld op 20 oktober 2020, p. 15.

voor de verwerking te kiezen en door te voeren dat er standaard uitsluitend verwerkingen worden uitgevoerd die strikt noodzakelijk zijn voor het gestelde, wettige doel.[119]

309. De EDPB wijst erop dat als de verwerkingsverantwoordelijke software van derden of in de handel verkrijgbare software gebruikt, hij een risicobeoordeling voor het betreffende product moet uitvoeren en er moet voor zorgen dat functies die geen rechtsgrond hebben of niet stroken met het beoogde doel van de verwerking, uitgeschakeld zijn. Volgens de EDPB moet hiermee in het bijzonder rekening worden gehouden bij het verlenen van toegang tot de gegevens aan personeelsleden met verschillende functies en verschillende toegangsbehoeften.[120]

310. In alle fasen van het ontwerp van de verwerkingsactiviteiten, inclusief inkoop, aanbestedingen, uitbesteding, ontwikkeling, ondersteuning, onderhoud, testen, opslag, vernietiging enz., moet de verwerkingsverantwoordelijke de verschillende elementen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen in acht en in overweging nemen.

311. Belangrijke ontwerp- en standaardinstellingselementen voor minimale gegevensverwerking zijn volgens de EDPB onder meer:[121]

> "- Gegevensvermijding – vermijd de verwerking van persoonsgegevens volledig wanneer dit mogelijk is voor het betreffende doel.
> - Beperking – beperk de hoeveelheid verzamelde gegevens tot wat noodzakelijk is voor het doel.
> - Beperking van toegang – geef de gegevensverwerking zo vorm dat zo weinig mogelijk mensen toegang tot persoonsgegevens nodig hebben om hun werkzaamheden uit te voeren, en beperk de toegang dienovereenkomstig.
> - Relevantie – persoonsgegevens zijn relevant voor de desbetreffende verwerking, en de verwerkingsverantwoordelijke kan deze relevantie aantonen.
> - Noodzakelijkheid – elke categorie van de persoonsgegevens is noodzakelijk voor de gespecificeerde doeleinden en wordt uitsluitend verwerkt indien het niet mogelijk is het doel met andere middelen te bereiken.
> - Aggregatie – gebruik waar mogelijk geaggregeerde gegevens.
> - Pseudonimisering – pseudonimiseer persoonsgegevens zodra het niet langer noodzakelijk is om over rechtstreeks identificeerbare persoonsgegevens te beschikken, en bewaar identificatiesleutels afzonderlijk.
> - Anonimisering en vernietiging – indien persoonsgegevens niet of niet langer noodzakelijk zijn voor het doel, worden deze geanonimiseerd of vernietigd.
> - Gegevensstroom – de gegevensstroom is voldoende doeltreffend, zodat er niet meer kopieën worden gemaakt dan noodzakelijk.

[119] EDPB, 'Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaard-instellingen', versie 2.0, vastgesteld op 20 oktober 2020, p. 13.
[120] EDPB, 'Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaard-instellingen', versie 2.0, vastgesteld op 20 oktober 2020, p. 13.
[121] EDPB, 'Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaard-instellingen', versie 2.0, vastgesteld op 20 oktober 2020, p. 24 e.v.

- "Stand van de techniek" – de verwerkingsverantwoordelijke past actuele en geschikte technologieën voor gegevensvermijding en minimale gegevensverwerking toe."

312. Belangrijke ontwerp- en standaardinstellingselementen voor integriteit en vertrouwelijkheid (beveiliging) zijn onder meer:[122]

"- Beheersysteem voor informatiebeveiliging (ISMS) – over operationele middelen beschikken om beleidslijnen en procedures voor informatiebeveiliging te beheren.
- Risicoanalyse – de risico's beoordelen aan de hand van de beveiliging van persoonsgegevens door na te denken over de gevolgen voor de rechten van individuen, en vastgestelde risico's tegengaan. Ontwikkel en onderhoud voor de risicobeoordelingen een uitgebreid, systematisch en realistisch dreigingsmodel en een analyse van het aanvalsoppervlak van de ontworpen software om de aanvalsvectoren de mogelijkheden om gebruik te maken van zwakke punten en kwetsbaarheden te beperken.
- Beveiliging door ontwerp – denk bij het ontwerp en de ontwikkeling van het systeem zo vroeg mogelijk na over beveiligingseisen en integreer en verricht voortdurend relevante tests.
- Onderhoud – evalueer en test software, hardware, systemen, diensten enz. regelmatig om kwetsbaarheden vast te stellen van de systemen die de verwerking ondersteunen.
- Beheer van toegangscontrole – enkel bevoegde medewerkers voor wie dit noodzakelijk is, hebben toegang tot de persoonsgegevens die zij nodig hebben voor hun verwerkingstaken, en de verwerkingsverantwoordelijke maakt onderscheid tussen de verschillende toegangsrechten van de bevoegde medewerkers.
- Beperking van toegang (personen) – geef de gegevensverwerking zo vorm dat zo weinig mogelijk mensen toegang tot persoonsgegevens nodig hebben om hun werkzaamheden te kunnen uitvoeren, en beperk de toegang dienovereenkomstig.
- Beperking van toegang (inhoud) – houd, in het kader van elke verwerkingsactiviteit, de toegang beperkt tot de gegevenskenmerken van de betreffende dataset die nodig zijn voor die activiteit. Beperk de toegang bovendien tot de gegevens die betrekking hebben op de betrokkenen die binnen het mandaat van de betreffende medewerker vallen.
- Segregatie van toegang – geef de gegevensverwerking zo vorm dat niemand volledige toegang tot alle verzamelde gegevens over een betrokkene nodig heeft, laat staan tot alle persoonsgegevens van een bepaalde categorie betrokkenen.
- Pseudonimisering – persoonsgegevens en back-ups/logbestanden worden gepseudonimiseerd als een beveiligingsmaatregel om de risico's van potentiële gegevensinbreuken tot een minimum te beperken, bijvoorbeeld door middel van hashing of versleuteling.
- Back-ups/logbestanden – houd back-ups en logbestanden bij voor zover dit noodzakelijk is voor informatiebeveiliging, en gebruik controlesporen en toezicht op gebeurtenissen als routinebeveiligingscontrole. Deze zaken moeten worden beschermd tegen ongeoorloofde en onbedoelde toegang en wijzigingen en moeten regelmatig worden herzien. Incidenten moeten onverwijld worden afgehandeld.
- Bescherming op basis van risico – bescherm alle categorieën persoonsgegevens met maatregelen die passen bij het risico van een beveiligingsinbreuk. Gegevens met bijzondere risico's moeten, indien mogelijk, apart van de rest van de persoonsgegevens worden bewaard.

[122] EDPB, 'Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaard-instellingen', versie 2.0, vastgesteld op 20 oktober 2020, p. 30 e.v.

- Beheer van reactie op veiligheidsincidenten – beschikken over routines, procedures en middelen om gegevensinbreuken op te sporen, in te dammen, te behandelen, te melden en er lering uit te trekken."

313. Specifiek ten tijde van de coronacrisis was er volop aandacht voor het beginsel privacy-by-design. De EDPB bood zelfs een *design guide* aan voor softwareontwikkelaars in de opinie over het gebruik van locatiegegevens en *contact tracing apps*.[123] Deze aandacht was er ook in Nederland ten aanzien van de CoronaMelder-app. Na een mislukte *appathon*, waarin een aantal plannen voor apps gepresenteerd werd, besloot de minister zelf een app te ontwikkelen. Er werden twee *taskforces* en een multidisciplinaire begeleidingscommissie ingesteld, de Begeleidingscommissie Digitale Ondersteuning Bestrijding Covid-19. In deze begeleidingscommissie werkten epidemiologen, huisartsen, gedragswetenschappers, IT- en security-experts en experts op het gebied van grondrechten en fundamentele vrijheden samen. Wanneer de verslagen van de Begeleidingscommissie worden teruggelezen valt op dat naarmate de tijd verstrijkt en steeds meer nieuws over het GGD-datalek naar buiten komt, de beveiliging van CoronIT en HPZone (Lite) ook meer aan bod komt (**productie K.22**). Bijzonder wrang is dan ook dat de CoronaMelder-app een positief geëvalueerd *privacy-by-design*-product is geworden dat door 2,9 miljoen mensen op enig moment actief is gebruikt, terwijl de centrale infrastructuur van de GGD – die niet aan de vereisten voldoet - de persoonsgegevens bevat van meer dan 6,5 miljoen Gedupeerden. Deze veel grotere groep zou geprofiteerd hebben van de aandacht van de juridische en technische experts waar de CoronaMelder-app op kon rekenen.

314. Opvallend is verder dat de Begeleidingscommissie op 21 februari 2022 nog schrijft dat:

> "***Verbindingen naar Coron-IT: een bekende/beruchte kwetsbaarheid.***
> *De commissie heeft herhaaldelijk gewezen op de noodzaak om verbindingen tussen verschillende eenheden en databronnen extra en herhaaldelijk te controleren. Dat wordt vooralsnog niet systematisch gedaan*."

315. Zelfs of dat moment, ruim een jaar nadat het datalek aan het licht kwam, is CoronIT dus nog steeds niet zo ingeregeld dat de verbindingen veilig zijn.

4.2.6.1 Export- en printfunctionaliteiten

316. Met name ten aanzien van de export- en printfunctionaliteiten is het beginsel van *privacy-by-design* in het geheel niet toegepast. Met de export- en printfunctionaliteiten kunnen grote bestanden met persoonsgegevens in zijn geheel worden gedownload of geprint.[124] Daarbij bestaat ook de mogelijkheid een bepaalde selectie van gegevens te maken (**productie F.15**).

---

[123] EDPB, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, aangenomen op 21 april 2020.
[124] *Kamerstukken II* 2020/21, 27529, nr. 234, p. 9 (**productie D.2**).

317. CoronIT beschikt over een printfunctionaliteit en was toegankelijk voor 26.000 medewerkers. De printfunctionaliteit was volgens GGD GHOR met name aanwezig om lijsten te kunnen printen in het kader van de noodprocedures die gebruikt moeten worden als er een systeem- of internetstoring is.[125] Volgens GGD GHOR werd deze functionaliteit echter, afhankelijk van de locatie, voor verschillende doeleinden gebruikt. Onder andere door de portier/verkeersregelaar om te controleren of mensen die aankomen een afspraak hebben om te voorkomen dat mensen zonder afspraak in de keten kwamen (**productie F.15**). 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. Het uitzetten van de printfunctionaliteit heeft volgens GGD GHOR geen problemen opgeleverd voor het operationeel proces.[126] Het niet toepassen van het beginsel van *privacy-by-design* is opvallend, nu het systeem in 2020 is ontwikkeld.

318. HPzone Lite is in augustus 2020 geïmplementeerd. HPZone Lite heeft een export- en een printfunctionaliteit.

319. De exportfunctionaliteit was volgens GGD GHOR nodig om datasets te creëren zodat GGD-epidemiologen analyses en rapportages konden maken op basis van datasets. Dat zou nodig zijn voor clusteronderzoek en uitbraakbestrijding. Daarnaast was de functie volgens GGD GHOR nodig zodat GGD'en analyses konden maken ten behoeve van rapportages voor gemeenten in hun GGD-regio.[127] Ook werd de exportfunctionaliteit gebruikt voor het genereren van databestanden om werk te verdelen over de medewerkers.[128] Volgens GGD HOR werden de lijsten ook gebruikt om de prestaties van de organisatie te monitoren (voorbeeld: analyse tijdigheid BCO ten behoeve van artsen, epidemiologen en data-analisten) (**productie F.15**). De exportfunctionaliteit is op 25 januari 2021 uitgezet en daarna weer voor een beperkt aantal medewerkers beschikbaar gesteld (**productie G.7**).[129]

320. De printfunctionaliteit binnen HPZone Lite stelde medewerkers volgens GGD GHOR in staat om de informatie die op dat moment zichtbaar was op de pagina op te slaan als PDF. De printfunctionaliteit werd volgens GGD GHOR voornamelijk gebruikt voor het overdragen van dossiers aan een andere GGD. Ook kon de functionaliteit worden gebruikt om een werklijst te printen.[130] De printfunctionaliteit is op 30 januari 2021 uitgezet.[131]

321. Alle GGD-medewerkers hadden toegang tot de print- en exportfunctionaliteiten. Voor de uitvoering van de werkzaamheden van GGD-medewerkers was het echter niet noodzakelijk dat de betreffende functionaliteiten binnen CoronIT en HPZone Lite algemeen toegankelijk waren

125 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 4 (**productie D.2**).
126 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 23 (**productie D.2**).
127 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 22 (**productie D.2**).
128 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 23 (**productie D.2**).
129 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 23 (**productie D.2**).
130 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 23 (**productie D.2**).
131 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 23 (**productie D.2**).

voor alle medewerkers. Dat blijkt al uit het feit dat de functionaliteiten na de berichtgeving door RTL Nieuws simpelweg zijn uitgezet.

322. Het feit dat de functionaliteiten voor alle GGD-medewerkers algemeen toegankelijk waren en dat bovendien ongelimiteerde mogelijkheden bestonden om gegevens te downloaden en te printen, maakten dat CoronIT en HPZone Lite zeer kwetsbaar waren voor datalekken. Dat risico heeft zich dan ook verwezenlijkt. Met gebruik van deze functies hebben GGD-medewerkers (bijzondere) persoonsgegevens van betrokkenen gedownload, online te koop aangeboden en verkocht (paragraaf 3.1.3 en 3.1.10).

323. Uit een e-mailwisseling van de GGD Noord- en Oost Gelderland blijkt overigens dat ook na het uitzetten van de exportfunctie in HPZone Lite, gebruikers van het systeem er op werden gewezen dat het nog wel mogelijk was om de gegevens "*via kopiëren en plakken*" over te nemen (**productie G.44**). In een groei- en voortgangsdocument van 25 juni 2021 van GGD Haaglanden wordt als beveiligingsrisico van CoronIT en HPZone Lite geconstateerd dat "*printscreen en copy paste acties*" naar andere programma's uitgevoerd kunnen worden (**productie G.2**).

324. Zowel ten aanzien van CoronIT als HPZone (Lite) zijn pas na bekend worden van het GGD-datalek in januari 2021 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.

325. Ook de te ruime toegangsrechten en het gebrek aan adequate logging en monitoring zijn overigens aan te merken als veronachtzaming van de beginselen van *privacy-by-design* en *by-default*.

4.2.6.2 Zoekfunctionaliteit

326. De zoekfunctionaliteit in de GGD-systemen biedt mogelijkheden om op basis van minimale, algemeen bekende gegevens eenvoudig gericht naar personen en dossiers te zoeken. Door zoekfunctionaliteiten te beperken, bijvoorbeeld door zoeken enkel mogelijk te maken op basis van een combinatie van gegevens die niet voor iedereen bekend is, had het risico dat onbevoegd persoonsgegevens van een specifieke persoon werden opgezocht en ingezien, aanmerkelijk kunnen worden verminderd.

327. De NOS heeft op basis van de instructies voor GGD-medewerkers bevestigd dat CoronIT sinds het begin van de pandemie de mogelijkheid bevatte om binnen het systeem te zoeken op een persoon. Door deze ruime zoekmogelijkheid konden medewerkers snel testuitslagen vinden en werd voorkomen dat dubbele dossiers werden aangemaakt (**productie C.9**). Voor CoronIT is deze

zoekfunctie aangepast per 4 februari 2021. Om dossiers terug te vinden zonder het BSN te gebruiken is dan altijd een combinatie van persoonsgegevens noodzakelijk.[132]

328. Ook HPZone Lite beschikt over een zoekfunctionaliteit, waarmee het mogelijk is om op naam te zoeken naar mensen die voorkomen in BCO (**productie C.9**). De landelijke werkinstructie illustreert hoe gemakkelijk het is om personen binnen HPZone Lite op te zoeken (**productie G.3**, bijlage 8). Bij het openen van de HPZone Lite applicatie kunnen medewerkers op het beginscherm zoeken aan de hand van een HPZone-nummer. Maar ook zonder HPZone-nummer kunnen medewerkers personen opzoeken door te zoeken op onder andere "*BSN, naam of geboortedatum*".

329. In een planbeschrijving van GGD Haaglanden die ziet op de veiligheid van de GGD-systemen wordt ten aanzien van HPZone Lite aangegeven dat er een groot risico bestaat op misbruik en verlies van data als gevolg van beschikbaarheid van grote datasets door de zoekfunctionaliteit (**productie G.9**). In dat verband wordt als mogelijke maatregel voorgesteld om de zoekfunctionaliteit alleen aan een beperkt aantal rollen toe te wijzen en indien mogelijk ook de export- en printfunctionaliteiten te deactiveren en beschikbaar te stellen voor slechts vier geautoriseerde rollen.

330. De AP heeft geconstateerd dat pas naar aanleiding van de berichtgeving door RTL Nieuws in CoronIT de zoekfunctionaliteit is aangepast. Hierdoor was het niet meer mogelijk om enkel op achternaam of een combinatie van achternaam en geslacht of achternaam en geboortedatum de gegevens van een specifieke persoon op te zoeken. Ook zou in CoronIT de informatie die medewerkers kunnen zien naar aanleiding van een zoekactie zijn beperkt, zouden verdere beperkingen zijn aangebracht in de zoekresultaten en zou de logging van zoekacties nader geanalyseerd worden. Ook zou de functie "*download afsprakenoverzicht*" zijn uitgeschakeld (**productie G.7**).

331. Uit het onderzoek van de AP blijkt echter dat een vergelijkbare beperking van de zoekfunctionaliteit in HPZone Lite niet is aangebracht, volgens GGD GHOR vanwege technische beperkingen bij de leverancier (**productie K.1**). In het groei- en voortgangsdocument van 25 juni 2021 van GGD Haaglanden wordt ook nog steeds als beveiligingsrisico van HPZone Lite genoemd dat door alle gebruikers een query gedraaid kan worden die een lijst oplevert met namen en postcodes en "*tot voor kort*" ook BSN en geboortedatum (**productie G.2**).

332. Alle GGD-medewerkers hadden toegang tot de zoekfunctionaliteiten. Voor de uitvoering van de werkzaamheden van GGD-medewerkers was het echter niet noodzakelijk dat de zoekfunctionaliteit algemeen toegankelijk was voor alle medewerkers. Dat blijkt ten aanzien van CoronIT al uit het feit dat de functionaliteiten na de berichtgeving door RTL Nieuws zijn beperkt.

[132] *Kamerstukken II* 2020/21, 27529, nr. 234, p. 22 (**productie D.2**).

333. Door direct de zoekfunctie zo in te stellen dat niet alleen op naam maar op een combinatie van gegevens, bijvoorbeeld naam en BSN, gezocht kon worden, had op eenvoudige wijze voorkomen kunnen worden dat iedereen in het volledige systeem elke persoon kon opzoeken. De Betrokkene zou immers zelf gemakkelijk aan de telefoon gegevens kunnen verstrekken. Hier had ook de noodknopprocedure als *privacy-by-design*-maatregel kunnen worden ingevoerd (zie onder).

4.2.6.3 Autorisatie en noodknopprocedure: need to know vs. "alles voor iedereen inzichtelijk"

334. In paragraaf 4.2.4.3 kwam al de ruime toegang tot data in CoronIT aan de orde: "*alles voor iedereen inzichtelijk*". Toepassing van de noodknopprocedure of het *breaking-the-glass*-principe zou een eenvoudige maatregel zijn geweest van toepassing van het beginsel van *privacy-by-design* en *privacy-by-default*. De standaardinstelling zou in dat geval bijvoorbeeld regionale toegang zijn. Zou een GGD-medewerker toegang tot een andere regio willen dan had op de noodknop kunnen worden gedrukt en daarbij kort de reden voor toegang kunnen worden ingevuld, bijvoorbeeld dat de betrokkene in de andere regio een afspraak had gemaakt maar deze toch liever verzet naar de eigen regio. Ook op functieniveau zou toegang beperkt kunnen zijn.

335. Door gebruik van de noodknopprocedure zou volledige toegang door iedereen technisch mogelijk zijn, maar zou achteraf goed te verklaren zijn waarom de toegang tot een bepaald dossier verkregen moest worden. Het zou de drempel tot het onrechtmatig opzoeken van bepaalde personen, aanmerkelijk hebben verhoogd. Ook zou het logging hebben vergemakkelijkt. Indien logging niet direct volledig mogelijk was, dan had het in de specifieke spoedeisende omstandigheden van de corona-epidemie in ieder geval direct op de noodknopprocedure kunnen worden toegepast.

336. Gelet op het voorgaande heeft de Staat c.s. in strijd gehandeld met de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen, zoals neergelegd in artikel 25 AVG.

4.2.7 Schending van de verantwoordingsplicht (artikel 5 lid 2 AVG en artikel 24 AVG)

337. Een verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de beginselen neergelegd in artikel 5 lid 1 AVG en moet dit kunnen aantonen (artikel 5 lid 2 AVG). In dat kader dient de verwerkingsverantwoordelijke ingevolge artikel 24 lid 1 AVG passende technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Die maatregelen moeten continu worden geëvalueerd en indien nodig geactualiseerd. De verwerkingsverantwoordelijke moet

kunnen aantonen dat elke verwerkingsactiviteit overeenkomstig de AVG geschiedt, ook wat betreft de doeltreffendheid van de maatregelen.[133]

338. Volgens de EDPB kan de verwerkingsverantwoordelijke in dat kader passende kernprestatie-indicatoren (KPI's) vaststellen om de doeltreffendheid aan te tonen:

> "Een KPI is een door de verwerkingsverantwoordelijke gekozen meetbare waarde die aantoont hoe doeltreffend de verwerkingsverantwoordelijke zijn doelstelling inzake gegevensbescherming verwezenlijkt. KPI's kunnen kwantitatief zijn, zoals het percentage valse positieven of valse negatieven, afname van klachten of vermindering van de reactietijd wanneer betrokkenen hun rechten uitoefenen, of kwalitatief, zoals beoordelingen van prestaties, gebruik van indelingsschema's of deskundige beoordelingen." [134]

339. In plaats van KPI's kan de verwerkingsverantwoordelijke volgens de EDPB de doeltreffende uitvoering van de beginselen ook aantonen door de gedachte achter zijn beoordeling van de doeltreffendheid van de gekozen maatregelen en waarborgen uiteen te zetten.

340. Artikel 24 lid 2 AVG werkt de verantwoordingsplicht verder uit door te bepalen dat een verwerkingsverantwoordelijke, wanneer dat in verhouding staat tot de verwerkingsactiviteiten, dient te beschikken over een passend gegevensbeschermingsbeleid dat ook uitgevoerd wordt.

341. De onbeperkte toegang tot persoonsgegevens en zoek, export- en printfunctionaliteiten en de afwezigheid van eenduidig beleid over het gebruik van eigen apparatuur, het toewijzen, wijzigen en intrekken van autorisaties, de controle van logging en screening van medewerkers duiden erop dat de Staat c.s. op geen enkele wijze hebben nagedacht over de naleving van de gegevensbeschermingsbeginselen, laat staan over de doeltreffendheid van dergelijke maatregelen.

342. Daarnaast hadden de Staat c.s., gezien de grootschalige verwerking van (bijzondere) persoonsgegevens, als onderdeel van het gegevensbeschermingsbeleid dienen te beschikken over een concreet (beveiligings)beleid c.q. een schriftelijke procedure met betrekking tot toegangsbeveiliging, autorisaties en autorisatiebeheer, logging en monitoring en screening en toezicht. Een dergelijk beveiligingsbeleid werd echter niet gehanteerd. Voor zover er enig beleid aanwezig was, staat vast dat dit in de praktijk niet (juist) werd uitgevoerd.

343. De AP heeft in dat verband ook geconstateerd dat er geen eenduidig beleid is vastgesteld over het gebruik van eigen apparatuur, geen duidelijke gedocumenteerde afspraken tussen de betrokken partijen zijn aangetroffen voor het toewijzen, wijzigen en intrekken van autorisaties en geen toereikende documentatie die ten aanzien van HPZone (Lite) inzichtelijk maakt welke specifieke rechten en functionaliteiten aan de verschillende rollen in de autorisatiematrix zijn

---

133 Overweging 74 AVG.

134 EDPB, 'Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaard-instellingen', versie 2.0, vastgesteld op 20 oktober 2020, p. 8.

gekoppeld. Tot slot was er volgens de AP geen sprake van beleid ten aanzien van de controle van logging (**productie K.1**).

344. De Staat c.s. heeft daarmee in strijd gehandeld met de verantwoordingsplicht, zoals neergelegd in artikel 5 lid 2 AVG en artikel 24 AVG.

4.2.8 Schending van de verplichting tot het uitvoeren van DPIA's

345. Een DPIA (een *data protection impact assessment,* in de woorden van de AVG een "gegevensbeschermingseffectbeoordeling") is een proces dat is bedoeld om de verwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid ervan te beoordelen en de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen te helpen beheren door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken. DPIA's zijn belangrijke verantwoordingsinstrumenten omdat ze verwerkingsverantwoordelijken niet alleen helpen om aan de eisen van de AVG te voldoen, maar ook om aan te tonen dat passende maatregelen zijn genomen teneinde ervoor te zorgen dat de AVG wordt nageleefd.[135] Met het resultaat van de beoordeling dient rekening te worden gehouden bij het bepalen van de passende maatregelen die moeten worden genomen om aan te tonen dat de AVG bij de verwerking van persoonsgegevens wordt nageleefd.[136]

346. Artikel 35 lid 1 AVG stelt een DPIA verplicht wanneer de verwerking gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Lid 2 sub b bepaalt dat een DPIA met name vereist is wanneer sprake is van een grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9 lid 1 AVG, zoals gezondheidsgegevens. De DPIA dient uitgevoerd te worden vóórdat de verwerking plaatsvindt.

347. In het Besluit van de AP inzake verwerkingen van persoonsgegevens waarvoor een DPIA verplicht is, wordt bevestigd dat dit het geval is bij grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratiebedrijven, (speciaal)onderwijs-instellingen, verzekeraars, en onderzoeksinstituten) waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid.[137]

348. Het staat dan ook vast dat de Staat c.s. een DPIA hadden moeten uitvoeren ten aanzien van de verwerking van gegevens in de GGD-systemen, en wel voorafgaand aan die verwerkingen. Dat

---

135 Groep gegevensbescherming artikel 29, 'Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679', vastgesteld op 4 oktober 2017, p. 4.

136 Overweging 84 bij de AVG.

137 Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermings-effectbeoordeling (DPIA) verplicht is, *Stcrt.* 2019, nr. 64418 van 27 november 2019.

de Staat c.s. niet (tijdig) hebben voldaan aan deze verplichting, blijkt uit de documentatie hierover:

a) Uit de datumaanduiding van de Referentie-DPIA-CoronIT (de datum staat niet in de DPIA zelf, maar op basis van de bestandnaam is de aanname dat de datum 26 maart 2021 is) kan worden afgeleid dat de Staat c.s. niet tijdig hebben gehandeld en hiermee de plicht hebben geschonden om een DPIA (tijdig) te verrichten (**productie G.1**). CoronIT wordt al sinds maart 2020 ingezet voor de bestrijding van de coronapandemie;

b) Uit de oplegnotitie DPIA Testen van de GGD Rotterdam-Rijnmond d.d. 17 juli 2020 blijkt ook dat gegevensbescherming en hiermee de (fundamentele) rechten van de burgers niet de prioriteit was van de Staat c.s. (**productie G.35**). Daarbij dient nog te worden opgemerkt dat, gelet op de bestandsnaam van het document (datumaanduiding 210617) alsmede de vergelijkbare inhoud met de oplegnotitie DPIA BCO van de GGD Rotterdam-Rijnmond d.d. 15 juli 2021, aannemelijk is dat de notitie van juli 2021 is, en niet van juli 2020;

c) Uit de oplegnotitie Voortgang DPIA's en privacyprogramma van de GGD Rotterdam-Rijnmond d.d. 7 oktober 2021 blijkt **(productie G.38**) dat de Staat c.s. niet tijdig de benodigde DPIA's hebben uitgevoerd. Zo staat daarin bijvoorbeeld ten aanzien van het de DPIA op het proces van bron- en contactonderzoek: *"DPIA op proces is nu volop gaande en bevindt zich door een update in de afrondende fase."*;

d) Ook uit de mailwisseling van GGD Rotterdam-Rijnmond d.d. 1 februari 2021 blijkt dat niet is voldaan aan de verplichting om een DPIA (volledig) te verrichten (**productie G.41**). In de mailwisseling wordt namelijk duidelijk dat ''d*e DPIA en Security maatregelen [voor CoronIT, adv.] zijn niet volledig uitgevoerd. [zwartgelakt]"*.

4.3 Overige schendingen

349. Op de GGD'en als zorgverlener is sectorspecifieke wetgeving van toepassing waarin, in aanvulling op de AVG, nadere regels gelden ten aanzien van onder andere het beroepsgeheim en de beveiliging van medische gegevens. In het hiernavolgende wordt uiteengezet dat de GGD'en inbreuk hebben gemaakt op artikel 7:457 BW, artikel 10 Wabvpz jo. artikel 2 Regeling gebruik burgerservicenummer in de zorg en artikel 15j Wabvpz jo. artikel 3 en 5 Begz.

4.3.1 GGD'en schenden artikel 7:457 BW (WGBO)

350. De WGBO is van toepassing op de overeenkomst inzake geneeskundige behandeling en regelt de rechten en plichten van patiënten. Ingevolge de WGBO dient de zorgaanbieder van iedere cliënt een medisch dossier bij te houden en te bewaren.

351. 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, anders dan met (expliciete) toestemming van de patiënt. De geheimhoudingsplicht ziet dus op zowel het verschaffen van inlichtingen als op het inzage verlenen in en afschrift geven van het medisch dossier aan derden. De weg waarlangs dit gebeurt is niet van belang.[138]

352. De geheimhoudingsplicht ten aanzien van medische gegevens vloeit eveneens voort uit artikel 7 Handvest en artikel 8 EVRM: het gebruik van medische gegevens zonder toestemming van de patiënt is een "*serious interference*" van het recht op privéleven.[139]

353. Uitgangspunt is dat iedereen die in de gezondheidszorg werkzaam is een geheimhoudingsplicht heeft. De geheimhoudingsplicht geldt dus niet alleen voor de individuele arts, maar ook voor de zorginstelling, die ervoor moet zorgen dat zijn medewerkers deze verplichting nakomen. Niet-medisch personeel heeft een afgeleid beroepsgeheim.[140]

354. Ingevolge artikel 7:457 lid 2 BW heeft de hulpverlener geen toestemming nodig van de patiënt als hij inlichtingen verstrekt aan personen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst. Het gaat hier bijvoorbeeld om doktersassistenten of een collega-vakgenoot die door de hulpverlener wordt geraadpleegd met het oog op de behandeling van de patiënt. Zelfs dan is van belang dat de gegevensverstrekking aan de betrokken andere hulpverlener niet verder mag gaan dan noodzakelijk is voor de te verrichten werkzaamheden.[141] Deze wijze van informatieverstrekking moet bovendien voor de patiënt kenbaar zijn en de patiënt heeft het recht om hiertegen bezwaar te maken (artikel 7:448 lid 1 BW).[142]

355. Bij het testen en vaccineren treden de GDD'en op als hulpverlener in de zin van artikel 7:457 BW.[143] De GGD'en hebben in dat kader een behandelingsovereenkomst met de Betrokkene, hetgeen door de GGD'en is bevestigd.[144] De GGD'en hebben daarnaast ook bevestigd dat zij op basis van een geneeskundige behandelingsovereenkomst gegevens, zoals corona-gerelateerde klachten en symptomen, vastleggen in het kader van BCO.[145] De GGD'en dienen derhalve geheimhouding te betrachten ten aanzien van de (medische) gegevens van patiënten. Desondanks hadden alle GGD-medewerkers toegang tot de persoonsgegevens in HPZone (Lite) en CoronIT. GGD-medewerkers hebben bovendien bevestigd dat zij toegang hadden tot gegevens in de GGD-systemen (van andere GGD-regio's) waar zij geen toegang tot zouden

138 R.P. Wijne, in: GS Bijzondere overeenkomsten, art. 7:457 BW, aant. 3 (online, bijgewerkt 2 maart 2022).
139 EHRM 25 februari 1997, zaaknr. 22009/93, par. 112 (Z./Finland); EHRM 17 juli 2008, zaaknr. 20511/03 (I./Finland) en EHRM 28 april 2009, zaaknr. 32881/04 (K.H. e.a/Slowakije).
140 R.P. Wijne, in: GS Bijzondere overeenkomsten, art. 7:457 BW, aant. 3 (online, bijgewerkt 2 maart 2022).
141 R.P. Wijne, in: GS Bijzondere overeenkomsten, art. 7:457 BW, aant. 8 (online, bijgewerkt 2 maart 2022).
142 KNMG-richtlijn, Omgaan met medische gegevens, KNMG, 2021, p. 16.
143 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 7-8 (**productie D.2**). Zie ook: Rechtbank Noord-Holland 12 april 2017, ECLI:NL:RBNHO:2017:2838.
144 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 7-8 (**productie D.2**).
145 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 49 (**productie D.2**).

moeten hebben (**productie C.8**). In dat verband heeft de AP eveneens vastgesteld dat diverse medewerkers over autorisaties beschikten die zij voor hun werkzaamheden niet of niet langer nodig hadden (**productie C.19**). De GGD'en hebben dientengevolge hun medische beroepsgeheim geschonden en bewerkstelligd dat de GGD-medewerkers hun beroepsgeheim niet zijn nagekomen. Zij hebben aldus gehandeld in strijd met de WGBO.

4.3.2 GGD'en handelen in strijd met de Wabvpz

356. De Wabvpz regelt onder meer wanneer en op welke wijze zorgaanbieders de identiteit van de cliënt dienen te controleren en op welke wijze ze het BSN van patiënten dienen vast te leggen. Artikel 8 Wabvpz legt zorgaanbieders de verplichting op om persoonsgegevens van hun cliënten te verbinden met hun BSN, voor zover de persoonsgegevens worden verwerkt in het kader van de verlening van zorg.

357. Ingevolge artikel 1 sub c Wabvpz is de zorgaanbieder overeenkomstig artikel 1 sub e Wkkgz een instelling dan wel een solistisch werkende zorgverlener. De zorgaanbieder kan de zorg doen verlenen door één of meer natuurlijke personen die bij hem in dienst zijn of door derden op een andere titel, bijvoorbeeld op basis van een toelatingsovereenkomst, een samenwerkings-overeenkomst of een overeenkomst van opdracht. De derde kan een (andere) rechtspersoon zijn.[146] Het begrip "zorg" is in artikel 1 onder b ruim gedefinieerd. Het omvat in beginsel alle wettelijk omschreven vormen van zorg en aanverwante diensten.[147] De definitie verwijst expliciet naar artikel 6b Wpg, namelijk het rijksvaccinatieprogramma waar corona onder valt.[148]

358. Volgens de GGD'en verrichten zij het testen en vaccineren in verband met corona als zorgverlener en heeft de GGD als zorgaanbieder de verplichting het BSN te registreren van Betrokkenen (**productie F.15**).[149] Testen, vaccineren en BCO zijn verrichtingen die ertoe strekken een persoon voor het ontstaan van een ziekte te behoeden en/of de gezondheidstoestand van een persoon te beoordelen. De Wabvpz is daarom van toepassing in het kader van het testen, vaccineren en BCO in verband met corona.

359. Op grond van artikel 10 Wabvpz kan bij ministeriële regeling worden bepaald aan welke beveiligingseisen de verwerking van het BSN, bedoeld in artikel 8 Wabvpz moet voldoen. Deze beveiligingseisen zijn uitgewerkt in de Regeling gebruik burgerservicenummer in de zorg. Ingevolge artikel 2 Regeling gebruik burgerservicenummer in de zorg moet de verwerking van het BSN door zorgaanbieders als bedoeld in artikel 8 Wabvpz voldoen aan de NEN 7510.

360. Daarnaast bepaalt artikel 15j Wabvpz dat bij algemene maatregel van bestuur regels kunnen worden gesteld over de functionele, technische en organisatorische maatregelen voor het

146 Van den Ende, in: T&C Gezondheidsrecht, commentaar op art. 1 WKKGZ (online, bijgewerkt 20 mei 2022).
147 *Kamerstukken II* 2005/06, 30 380, nr. 3, p. 13-18 (*MvT*).
148 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 61 (**productie D.2**).
149 *Kamerstukken II* 2020/21, 27529, nr. 234, p. 70 (**productie D.2**).

beheer, de beveiliging en het gebruik van een zorginformatiesysteem of een elektronisch uitwisselingssysteem. Deze regels zijn uitgewerkt in de Begz. Op grond van artikel 3 lid 2 en artikel 5 lid 1 van het Begz dient een zorgaanbieder bij de beveiliging en de logging van zijn zorginformatiesysteem te handelen overeenkomstig het bepaalde in NEN 7510 en NEN 7513. Ingevolge artikel 3 lid 2 Begz draagt een zorgaanbieder, overeenkomstig het bepaalde in NEN 7510 en NEN 7512, zorg voor een veilig en zorgvuldig gebruik van het zorginformatiesysteem en een veilig en zorgvuldig gebruik van het elektronisch uitwisselingssysteem waarop hij is aangesloten.

361. Volgens GGD GHOR is CoronIT "*een zorginformatiesysteem en geen elektronisch uitwisselingssysteem, omdat het niet gebruikt wordt om dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar te kunnen maken*."[150] Ook HPZone (Lite) is een zorginformatiesysteem aangezien het werd gebruikt voor het (elektronisch) verwerken van persoonsgegevens in een dossier ten behoeve van het bron- en contactonderzoek. Het gebruik van beide systemen moeten daarom voldoen aan NEN 7510.

362. Overeenkomstig artikel 5 lid 1 Begz draagt de zorgaanbieder er tevens zorg voor dat de logging van het systeem voldoet aan het bepaalde in NEN 7513. NEN 7513 vult NEN 7510 nader in als het gaat om logging.

363. De GGD'en hebben niet voldaan aan de normen uit de NEN 7510, de NEN 7512 en de NEN 7513, zoals hiervoor uiteengezet. Zij hebben daarmee aldus niet enkel in strijd gehandeld met de AVG, maar ook met de Wabvpz.

5 SCHADE

364. Het GGD-datalek heeft plaatsgevonden en de Gedupeerden zijn daardoor permanent de controle over hun persoonsgegevens verloren. Dat kan niet meer worden teruggedraaid. De Gedupeerden lijden daardoor schade en Stichting ICAM c.s. menen meent dat een collectieve schadevordering het enige gepaste middel is om de Gedupeerden te compenseren. Naast vergoeding van daadwerkelijk geleden (im)materiële schade, heeft deze vordering als bijkomend doel dat de Staat c.s. tot verantwoording worden geroepen voor het GGD-datalek. Stichting ICAM beoogt met het instellen van deze geldvordering dat de Staat c.s. zullen inzien dat er een urgente noodzaak bestaat tot verbetering van de bescherming van persoonsgegevens van burgers.

365. Stichting ICAM meent daarom dat in deze zaak ruimhartig schade dient te worden toegewezen. Zij zal dat standpunt inleiden met een bespreking van het belang van civielrechtelijke handhaving van de AVG (paragraaf 5.1). Vervolgens bespreekt Stichting ICAM het toetsingskader voor immateriële schadevergoedingsvorderingen (paragraaf 5.2), waarbij zij primair zal betogen dat de AVG een zelfstandige en autonoom uit te leggen grondslag biedt voor schadevergoeding

[150] *Kamerstukken II* 2020/21, 27529, nr. 234, p. 55 (**productie D.2**).

(paragraaf 5.2.1). Subsidiair, voor zover de rechtbank van oordeel is dat aangesloten moet worden bij het Nederlandse schadevergoedingsrecht, stelt Stichting ICAM zich op het standpunt dat dit, voor zover nodig, EU-conform dient te worden uitgelegd en dus niet zal leiden tot andere conclusies. Uit de nationale rechtspraak blijkt ook dat Nederlandse rechters doorgaans immateriële schadevergoeding toekennen op een wijze die in lijn is met de doelstellingen van de AVG. Daarbij is relevant dat de AVG geen materiële ondergrens kent voor de toekenning van schadevergoeding en dat in deze zaak sprake is van zodanig onrechtmatig handelen dat de nadelige gevolgen daarvan, gelet op de aard en de ernst van de normschending, zo duidelijk zijn dat persoonlijke aantasting mag worden aangenomen (paragraaf 5.2.2). Vervolgens bespreekt Stichting ICAM de immateriële schade zoals de Gedupeerden die hebben geleden (paragraaf 5.3) en de wijze waarop de omvang daarvan middels tarifering moet worden bepaald (paragraaf 5.3.2). Ten slotte wordt uiteengezet welke materiële schade de Gedupeerden hebben geleden (paragraaf 5.4).

5.1 Ter inleiding: ruim baan voor privaatrechtelijke handhaving van de AVG

366. Zowel bij de beoordeling van de ernst van de overtredingen als bij het vaststellen van het bestaan van een schadevergoedingsplicht en de omvang van de schade, dient acht te worden geslagen op de achtergrond van het recht op schadevergoeding zoals dat voortvloeit uit de AVG.

367. De Uniewetgever heeft met de AVG beoogd Betrokkenen een hoog beschermingsniveau te bieden en een doeltreffende bescherming van persoonsgegevens te waarborgen. Handhaving maakt daarvan een belangrijk onderdeel uit. De AVG verplicht lidstaten een systeem toe te passen dat zorgt voor "*doeltreffende, evenredige en afschrikkende*" sancties.[151] Overweging 7 vermeldt dat het gegevensbeschermingskader "*moet worden ondersteund door een krachtige handhaving*". Het belang van krachtige handhaving komt ook tot uiting in het uitgebreide arsenaal handhavingsinstrumenten in de AVG. Overtreding kan resulteren in boetes tot € 10.000.000,- of € 20.000.000,-, respectievelijk 2% of 4% van de wereldwijde jaaromzet (artikel 83 AVG).

368. Nationale toezichthouders, waaronder de AP, beschikken echter niet over voldoende capaciteit om op schendingen te reageren (**productie C.31 en C.32**). Dit was een bekend probleem vóór inwerkingtreding van de AVG en is sindsdien alleen maar nijpender geworden. Serieuze boetes worden maar zelden opgelegd, terwijl de AP 27.800 klachten ontving in 2019, 25.500 klachten in 2020 en 27.850 klachten in 2021. Het is voor de AP onmogelijk om op al deze klachten te reageren (**producties C.33 t/m C.36**). De AP heeft ook zelf aangegeven dat zij onvoldoende capaciteit heeft (**productie C.35**). In een AVG-evaluatierapport van de Europese Commissie uit de Commissie zorgen over het nadelige effect hiervan op handhaving van de AVG.[152]

[151] Artikel 84 AVG en overweging 151 en 152 bij de AVG
[152] Europese Commissie, 27 juni 2020, 'Staff Working Document: accompanying the Communication - two years of application of the General Data Protection Regulation (COM(2020) 264 final).

369. Gelet op deze achtergrond dient in deze zaak rekening te worden gehouden met het belang van privaatrechtelijke handhaving. Wanneer een grove schending van het gegevensbeschermingsrecht niet leidt tot serieuze bestuursrechtelijke sancties, is effectieve, volledige en doeltreffende civielrechtelijke handhaving noodzakelijk. Het kunnen handhaven van de belangrijkste beginselen van de AVG en de rechten van Betrokkenen is essentieel voor een doeltreffende bescherming van persoonsgegevens.

370. Privaatrechtelijke handhaving heeft mede daarom een prominente plaats in de AVG en steeds meer actoren dringen aan op krachtige civiele handhaving tegen schendingen.[153]

371. Ook het HvJEU heeft benadrukt dat het recht op schadevergoeding kan bijdragen tot de "volle werking" van het recht van de Unie.[154] In een aantal zaken over inbreuken op het mededingingsrecht heeft het HvJEU overwogen dat het recht op schadevergoeding inbreuken "*minder aantrekkelijk*" maakt en kan bijdragen tot "*daadwerkelijke mededinging*".

372. De mogelijkheid om schadevergoeding te eisen zal op soortgelijke wijze schendingen van de AVG ontmoedigen en bijdragen tot de handhaving ervan.[155] Een hoge drempel voor het vergoeden van schade bij schendingen van de AVG zou het "handhavingstekort" niet verminderen.[156]

373. In zijn conclusie bij het *EBI*-arrest bespreekt A-G Hartlief – daarbij uitgebreid verwijzend naar literatuur – de ontwikkeling van het recht op immateriële schadevergoeding, mede in het licht van handhaving als één van de functies van het schadevergoedingsrecht. Hij betoogt dat het zich niet goed met de aard van fundamentele rechten verdraagt wanneer een schending alleen tot compensatie zou leiden indien de benadeelde daarvan (concrete, aanwijsbare) gevolgen heeft ondervonden. Het gaat immers juist om waarden en belangen die tamelijk “ongrijpbaar” zijn, zodat de gevolgen van een schending moeilijk kunnen worden geobjectiveerd en die juist

---

153 T.F. Walree, 'De vergoedbare schade bij een onrechtmatige verwerking van persoonsgegevens', *WPNR* 2017/7172, p. 921; E. O'Dell, 'Compensation for Breach of the General Data Protection Regulation', Dublin: Dublin University Law Journal 2017/40(1), 97-164; E. Truli, 'The General Data Protection Regulation and Civil Liability', in: *Persoonsgegevens in het mededingings-, consumentenbeschermings- en intellectuele eigendomsrecht*, M. Bakhoum e.a. (red.), Springer-Verlag 2018, p. 310; E.F.D. Engelhard, 'Immateriële schade als gevolg van data-inbreuken: het ondergeschoven kindje van de AVG', *NTBR* 2019/30, aflevering 9/10, p. 194.

154 HvJ EG 20 september 2001, C-453/99, ECLI:EU:C:2001:465, r.o. 25-27 (*Courage/Crehan*); HvJ EG 13 juli 2006, C-295/04-C-298/04, ECLI:EU:C:2006:461, r.o. 89-91 (*Manfredi*); HvJ EG 6 november 2012, C-199/11, ECLI:EU:C:2012:684, r.o. 41-42 (*Europese Gemeenschap/Otis e.a.*); HvJ 6 juni 2013, C-536/11, ECLI:EU:C:2013:366, r.o. 22-23 (*Donau Chemie e.a.*); HvJ EU 5 juni 2014, C-557/12, ECLI:EU:C:2014:1317, r.o. 21-23 (*Kone*); HvJ EU 14 maart 2019, C-724/17, ECLI:EU:C:2019:204, r.o. 43-45 (*Skanska*); HvJ EU 12 december 2019, C-435/18, ECLI:EU:C:2019:1069, r.o. 22-24 (*Otis e.a./Land Oberösterreich e.a.*).

155 E. Truli, 'De Algemene verordening gegevensbescherming en civielrechtelijke aansprakelijkheid', in: *Persoonsgegevens in Mededinging, Consumentenbescherming en Intellectueel Eigendomsrecht*, M. Bakhoum e.a. (red.), Springer-Verlag 2018, p. 310; T.F. Walree & P.T.J.Wolters, 'Het recht op schadevergoeding van een concurrent bij een schending van de AVG',SEW 2020/1, p. 7. Zie ook M.M.A. Janssen, *Persoonsgegevens en immateriële schade*, Weert: Celsus 2021, p. 21, waar zij de functies achter het voorzien in een recht op schadevergoeding uiteenzet, waaronder de preventieve functie.

156 T.E. van der Linden & T.F. Walree, 'De collectieve procedure als oplossing voor het privaatrechtelijke handhavingstekort bij een datalek?', *AV&S 2018/20*, aflevering 4, p. 105-113.

(daarom) op zichzelf bescherming behoeven.[157] Ook AVG-inbreuken hebben naar hun aard vaak geen bewijsbare concrete gevolgen. Voor de doeltreffendheid van het recht van de Unie is het daarom van belang dat de drempel voor toekenning van immateriële schadevergoeding niet te hoog is, zoals bijvoorbeeld het geval kan zijn bij een te beperkte invulling van het begrip immateriële schade in artikel 82 AVG. Hartlief benadrukt ook dat de suggestie is dat het bij smartengeld wegens schending van fundamentele rechten steeds zou moeten gaan om ernstige inbreuken en de gevolgen daarvan voor de rechthebbende. Hartlief meent echter dat het wel degelijk ook kan gaan om gevallen waarin deze lat juist niet zo hoog wordt gelegd, zoals bij de redelijke termijn-rechtspraak.[158]

374. Gebleken is dat Betrokkenen zelden individuele schadevergoedingsacties aanhangig maken tegen verwerkingsverantwoordelijken.[159] Over het algemeen is de individuele schade bij een datalek namelijk gering, in tegenstelling tot de schadepost van de gehele groep van Gedupeerden. Voor het individu is een schadeactie tegen een verwerkingsverantwoordelijke dan ook oneconomisch en irrationeel.[160] Om die reden is van belang dat collectieve belangenorganisaties, zoals Stichting ICAM, in rechte voor een groep Betrokkenen op kunnen komen en namens hen schadevergoeding kunnen vorderen.

375. De AVG voorziet dan ook ruimschoots in de mogelijkheid tot (collectieve) civielrechtelijke handhaving:

a) Artikel 80 AVG geeft betrokkenen de mogelijkheid zich te laten vertegenwoordigen door een belangenorganisatie die namens hen bepaalde rechten uitoefent en het recht op schadevergoeding uitoefent;

b) Artikel 82 AVG geeft eenieder die schade heeft geleden door een schending van de AVG het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen.

376. Stichting ICAM c.s. zullen in paragraaf 5.2.1 ingaan op de invulling van het schadebegrip in artikel 82 AVG. In paragraaf 9.2 zullen zij ingaan op de verhouding tussen artikel 80 AVG en de mogelijkheden die de WAMCA biedt om collectief schade te vorderen.

[157] Conclusie A-G 16 oktober 2018, ECLI:NL:PHR:2018:1295, par. 4.1 t/m 4.60 en met name 4.49.
[158] Conclusie A-G 16 oktober 2018, ECLI:NL:PHR:2018:1295, par. 4.49.
[159] T.F. Walree, *Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens,* (O&R nr. 126), diss. Nijmegen, Deventer: Wolters Kluwer 2021, p. 34.
[160] T.F. Walree, Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens, (O&R nr. 126), diss. Nijmegen, Deventer: Wolters Kluwer 2021, p. 40-41.

5.2 Toetsingskader immateriële schadevergoedingsvorderingen

5.2.1 Primair: vergoeding van immateriële schade onder artikel 82 AVG

377. Artikel 82 AVG bepaalt expliciet dat eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op de AVG, recht heeft op vergoeding van die schade:

> "Eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op deze verordening, heeft het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade."

378. Artikel 82 lid 1 AVG biedt een zelfstandige Europeesrechtelijke grondslag voor toekenning van schadevergoeding aan de Gedupeerden. Anders dan andere Unierechtelijke instrumenten die voorzien in een recht op schadevergoeding, bepaalt artikel 82 AVG immers niet dat het begrip "schade" aan de hand van het nationale recht moet worden uitgelegd. Nu artikel 82 AVG niet nadrukkelijk verwijst naar het recht van de lidstaten, dient het autonoom en uniform te worden uitgelegd, ten behoeve van de eenvormige toepassing van het Unierecht en het gelijkheidsbeginsel.[161] Deze plicht tot autonome uitleg brengt met zich mee dat nationaal recht geen afbreuk kan doen aan het bepaalde in dit artikel en dat de nationale rechter de volle werking van artikel 82 AVG en de daarin aan particulieren toegekende rechten moet beschermen.[162] De autonome uitleg van artikel 82 AVG heeft voorrang op een eventuele afwijkende nationale interpretatie van het schadebegrip.[163]

379. Overweging 146 bij de AVG licht toe dat alle schade die iemand kan lijden ten gevolge van een inbreuk op de AVG volledig en daadwerkelijk moet worden vergoed, en dat het begrip "schade" ruim moet worden uitgelegd:

> "De verwerkingsverantwoordelijke of de verwerker moeten alle schade vergoeden die iemand kan lijden ten gevolge van een verwerking die inbreuk maakt op deze verordening. De verwerkingsverantwoordelijke of de verwerker moet van zijn aansprakelijkheid worden vrijgesteld indien hij bewijst dat hij niet verantwoordelijk is voor de schade. Het begrip „schade" moet ruim worden uitgelegd in het licht van de rechtspraak van het Hof van Justitie, op een wijze die ten volle recht doet aan de doelstellingen van deze verordening. […] De betrokkenen dienen volledige en daadwerkelijke vergoeding van door hen geleden schade te ontvangen […]"

380. Een ruim schadebegrip strookt met name ten aanzien van immateriële schade met het doel van de AVG. Inbreuken op de AVG resulteren voor Betrokkenen immers vaak uitsluitend of voornamelijk in immateriële schade en/of in schade die in de toekomst is gelegen en waarvan

---

161 Vgl. HvJEU 18 oktober 2011, ECLI:EU:C:2011:669 (*Brüstle/Greenpeace*), r.o. 25; HvJEU 14 februari 2012, ECLI:EU:C:2012:71 (*Flachglas Torgau/Duitsland*), r.o. 37; HvJEU 19 december 2013, C-279/12, ECLI:EU:C:2013:853 (*Fish Legal/Information Commissioner*), r.o. 42.

162 HvJ EG 9 maart 1978, ECLI:EU:C:1978:49 (*Simmenthal*), r.o. 21

163 Zie T.F. Walree, *Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens,* (O&R nr. 126), diss. Nijmegen, Deventer: Wolters Kluwer 2021, p.117 en 118 en de daar vermelde rechtspraak en literatuur.

moeilijk kan worden aangetoond dat die in causaal verband staat tot de overtreding. Indien immateriële schade ten gevolge van AVG-schendingen niet ruimhartig wordt toegekend, wordt civiele handhaving van de normen uit de AVG tandeloos, en daarmee die normen zelf voor een groot deel ook (zie ook paragraaf 5.1 en 6.2.5.1).

381. Overweging 146 licht ook toe dat het begrip “schade” dient te worden uitgelegd in het licht van de rechtspraak van het HvJEU, op een wijze die ten volle recht doet aan de doelstellingen van de AVG. Voor wat betreft het recht op vergoeding van immateriële schade leidt dat tot de volgende analyse.

5.2.1.1 Controle over persoonsgegevens als doelstelling van de AVG

382. In overweging 75 en 85 AVG overweegt de EU-wetgever expliciet dat Betrokkenen immateriële schade kunnen lijden als gevolg van het verlies van controle over hun persoonsgegevens. Wat "verlies van controle" inhoudt, wordt niet uitgelegd in de AVG. Een enge interpretatie is dat het zich voordoet wanneer een niet-bevoegde partij persoonsgegevens van de Betrokkene verwerkt. Een dergelijke enge interpretatie doet echter geen recht aan het hoge niveau van bescherming dat de AVG beoogt te bieden.[164]

383. Een door onder andere Walree voorgestane ruime interpretatie, die wel recht doet aan het beschermingsniveau van de AVG, is de volgende.[165] Indien de verwerkingsverantwoordelijke niet voldoet aan de belangrijkste beginselen van de AVG - waaronder transparantie, doelbinding, gegevensminimalisering, nauwkeurigheid, integriteit, opslagbeperking en vertrouwelijkheid - kan de Betrokkene niet effectief controleren of zijn persoonsgegevens rechtmatig worden verwerkt en kan hij ernstig worden beperkt in de uitoefening en handhaving van zijn rechten. In die zin verliest de Betrokkene de controle over zijn persoonsgegevens door het loutere feit dat de verwerkingsverantwoordelijke de AVG-beginselen niet in acht heeft genomen. In dit verband licht overweging 63 bij de AVG toe dat Betrokkenen de mogelijkheid moeten hebben om "kennis te nemen van de rechtmatigheid van de verwerking en deze te controleren".

384. In een tweetal uitspraken van 25 februari 2022 heeft de kantonrechter van de rechtbank Rotterdam een immateriële schadevergoeding van € 250,- toegekend wegens verlies van controle over persoonsgegevens. Gedaagde in beide procedures had per ongeluk een onbeveiligd Excelbestand rondgestuurd aan 1.100 personen die dat niet hadden moeten ontvangen met daarin de gegevens van de betreffende 1.100 Betrokkenen. Naast gegevens zoals voor- en achternaam, geboortedatum en –plaats en adres, bevatte de Excellijst ook financiële gegevens. De kantonrechter overwoog als volgt:

---

164 T.F. Walree, ‘De onrechtmatige verwerking van persoonsgegevens: geen concrete gevolgen, wel schadevergoeding?’ *RM Themis* 2020/4, p. 170.

165 T.F. Walree, ‘De onrechtmatige verwerking van persoonsgegevens: geen concrete gevolgen, wel schadevergoeding?’ *RM Themis* 2020/4, p. 171.

> "[gedaagde] heeft dus niet betwist dat de onrechtmatige verwerking tot vervelende gevolgen voor [eiseres] heeft geleid. Zij stelt zich echter op het standpunt dat dit geen juridisch relevante schade is, in de zin van artikel 6:106 lid 1 sub b BW. Zij gaat er echter aan voorbij dat artikel 82 AVG autonoom dient te worden uitgelegd op een wijze die ten volle recht doet aan de doelstellingen van deze verordening, zoals hiervoor overwogen onder r.o. 4.2. Naar oordeel van de kantonrechter kunnen de gevolgen die de onrechtmatige verwerking voor [eiseres] hebben gehad wel degelijk schade opleveren zoals bedoeld in artikel 82 AVG. Dat de schade op zichzelf niet direct gesubstantieerd kan worden, zoals door [gedaagde] aangevoerd, is daarvoor geen belemmering. Een van de hoofddoelen van de AVG is namelijk dat iedere persoon de controle houdt over zijn eigen persoonsgegevens (overweging 7 AVG). [eiseres] is deze controle kwijtgeraakt doordat [gedaagde] de gegevens heeft doorgestuurd naar een aanzienlijke groep mensen. Zoals [eiseres] tijdens de zitting onbetwist heeft aangevoerd is niet te achterhalen waar deze gegevens nu circuleren. In het kader van een doeltreffende naleving van de AVG is de kantonrechter van oordeel dat dit dient te worden aangemerkt als schade van [eiseres] ."

385. In het onderhavige geval hebben de Staat c.s. de persoonsgegevens van de Gedupeerden niet adequaat beveiligd. Als gevolg hiervan zijn persoonsgegevens voor onbevoegden toegankelijk geweest en ook daadwerkelijk gestolen. De Gedupeerden hebben daardoor geen controle meer over hun (bijzondere) persoonsgegevens. De Gedupeerden hebben immers geen invloed (meer) op waar persoonsgegevens terechtkomen en worden tevens beperkt in de uitoefening en handhaving van hun rechten onder de AVG.

5.2.1.2 Rechtspraak van het HvJEU

386. Het HvJEU heeft zich nog niet uitgelaten over het schadebegrip in artikel 82 AVG, in het bijzonder wat betreft de vergoeding van immateriële schade. Wel heeft het HvJEU op andere rechtsgebieden uitspraken gewezen met betrekking tot de vergoeding van immateriële schade.

387. In het *Europese Ombudsman*-arrest overwoog het HvJEU dat immateriële schade "reëel en zeker" moet zijn om voor vergoeding in aanmerking te komen.[166] Dit vereiste werpt echter geen hoge drempel op voor het aannemen van immateriële schade. In het arrest werd een "gevoel van psychologische schade" reeds als reële en zekere schade aangemerkt.[167] Daarbij baseerde het HvJEU zich op de subjectieve verklaring van eiser, in afwijking van het advies van de A-G.[168] In het *Gascogne*-arrest overwoog het Gerecht EU dat ook "een verlengde staat van onzekerheid" over de uitkomst van een gerechtelijke procedure en "gevoelens van onrust en onbehagen" reeds kunnen leiden tot immateriële schade.[169]

388. Het HvJEU heeft bovendien in meerdere uitspraken geoordeeld dat onrechtmatig gedrag onder bijzondere omstandigheden zo ernstig kan zijn, dat op basis van dat handelen aangenomen kan

[166] HvJEU 4 april 2017, C-337/15 P, ECLI:EU:C:2017:256, (*Europese Ombudsman/Staelen*), r.o. 91.
[167] HvJEU 4 april 2017, C-337/15 P, ECLI:EU:C:2017:256, (*Europese Ombudsman/Staelen*), r.o. 129 - 131.
[168] Conclusie AG 27 oktober 2016, C-337/15 (*Europese Ombudsman/Staelen),* par. 114.
[169] Gerecht EU 10 Januari 2017, T577/14, ECLI:EU:T:2017:1, paragraaf 151 *(Gascogne/Europese Unie*), r.o. 157.

worden dat sprake is van immateriële schade.[170] Die argumentatie komt ook in nader te bespreken Nederlandse rechtspraak terug. Ook deze drempel is laag. Ter illustratie oordeelde het Gerecht EU in het *Gascogne*-arrest dat de niet-inachtneming van de redelijke procestermijn reeds voldoende ernstig kan zijn.[171]

389. Een uitspraak van het Gerecht EU inzake *HJ/EMA* heeft wel betrekking op de vergoeding van immateriële schade wegens onvoldoende bescherming van persoonsgegevens. Het feitencomplex dat in deze zaak centraal stond komt er op neer dat het personeelsdossier van een werkneemster een maand lang toegankelijk was voor collega's. De werkneemster hoefde volgens het Gerecht EU niet te bewijzen dat collega's haar dossier daadwerkelijk hadden ingezien. Het enkele feit dat die mogelijkheid bestond was voldoende voor het aannemen van immateriële schade.[172]

390. Eenzelfde feitencomplex bestond in het arrest *I./Finland* van het EHRM. Het patiëntendossier van een voormalig werknemer, tevens patiënt, van een ziekenhuis was toegankelijk voor andere werknemers. Het EHRM oordeelde dat het ziekenhuis niet kon bewijzen wie toegang hadden gehad tot het dossier, waarmee zij ook niet kon vaststellen dat er geen onrechtmatige toegang was geweest. Nu het ziekenhuis geen adequate beveiligingsmaatregelen had genomen, schond zij daarmee artikel 8 EVRM. Het EHRM kende de gedupeerde een schadevergoeding van € 33.771,- toe.[173]

391. Laatstgenoemde twee zaken vertonen gelijkenissen met onderhavige zaak, in die zin dat met betrekking tot een groot deel van de Gedupeerden niet kan worden vastgesteld of er daadwerkelijk onrechtmatige toegang is geweest tot hun bijzondere persoonsgegevens. Of die toegang bewezen kan worden is echter onder verwijzing naar deze rechtspraak niet relevant.

5.2.1.3 Tussenconclusie: een lage drempel voor toekenning van immateriële schade

392. Uit het bovenstaande volgen twee belangrijke richtlijnen bij de beoordeling van een immateriële schadevordering onder de AVG en bij de uitleg van het immateriële schadebegrip in de AVG.

393. Ten eerste dient de nationale rechter de volle werking van door Unierecht aan particulieren toegekende rechten te verzekeren.[174] Dit brengt onder meer met zich mee dat Unierecht moet

[170] HvJEU 6 februari 1986, C-173/82, C-157/83 en C-186/84, ECLI:EU:C:1986:54, (*Castille/Commissie*); HvJEU 17 december 1998, T-203/96, ECLI:EU:T:1998:302, paragraaf 108 (*Ambassade/Europees Parlement*); HvJEU 8 januari 1999, T-230/95, ECLI:EU:T:1999:11, paragraaf 39 (*BAI/Commissie*); HvJEU16 juli 2009, C-481/07, ECLI:EU:C:2009:461, paragraaf 38 (*SELEX Sistemi Integrati/Commissie*); Gerecht EU 10 Januari 2017, T577/14, ECLI:EU:T:2017:1, paragraaf 151 *(Gascogne/Europese Unie*).

[171] Gerecht EU 10 Januari 2017, T577/14, ECLI:EU:T:2017:1, paragraaf 151 *(Gascogne/Europese Unie*), r.o. 157.

[172] Gerecht EU 15 januari 2019, T-881/16, ECLI:EU:T:2019:5 (*HJ/EMA*).

[173] EHRM 17 juli 2008, ECLI:CE:ECHR:2008:0717JUD002051103 *(I./Finland*).

[174] HvJEU 13 juli 2006, ECLI:EU:C:2006:461 (*Manfredi*), r.o. 87; HvJEU 20 september 2001, ECLI:EU:C:2001:465 (*Courage*), r.o. 25.

worden toegepast op zowel het recht op schadevergoeding als bij de uitleg van het schadebegrip. De AVG is een verordening en werkt dus direct door in de Nederlandse rechtsorde.

394. Ten tweede dient een lage drempel te worden gehanteerd bij het beoordelen van een schadevergoedingsplicht. Het HvJEU oordeelde immers dat reeds een "gevoel van psychische schade", "een verlengde staat van onzekerheid" en "gevoelens van onrust en onbehagen" als reële en zekere schade zijn aan te merken,[175] het Gerecht EU oordeelde dat het enkele feit dat een personeelsdossier toegankelijk was geweest voldoende was voor de toekenning van immateriële schade, zonder dat er bewijs hoefde te zijn dat onbevoegden daadwekelijk in het dossier hadden gekeken[176] en verschillende uitspraken laten zien dat het voldoende kan zijn dat de eiser aantoont dat het onrechtmatig handelen zodanig ernstig is, dat dit als zodanig immateriële schade kan veroorzaken, waarbij een lage drempel moet worden gehanteerd en waarbij het verder aantonen van nadeel dan niet is vereist.[177]

5.2.1.4 Prejudiciële vragen

395. Inmiddels hebben vijf nationale rechters prejudiciële vragen gesteld aan het HvJEU met betrekking tot de vergoeding van immateriële schade onder artikel 82 AVG.

396. Het Oostenrijkse *Oberste Gerichtshof* heeft het HvJEU drie vragen over de toepassing van artikel 82 AVG gesteld, die hieronder worden behandeld (paragraaf 5.2.1.5).[178]

397. De hoogste bestuursrechter in Bulgarije heeft prejudiciële vragen gesteld over immateriële schadevergoeding onder de AVG in het kader van een grootschalig datalek uit de systemen van de Bulgaarse Belastingdienst. De Bulgaarse bestuursrechter wenst onder meer te vernemen of enkel de zorgen, ongerustheid en angst over een mogelijk misbruik van persoonsgegevens een vordering tot immateriële schadevergoeding rechtvaardigt. Ook legt zij aan het HvJEU de vraag voor op wie de bewijslast rust dat beveiligingsmaatregelen uit hoofde van artikel 32 AVG (al dan niet) passend waren.[179]

398. Het Duitse *Bundesarbeitsgericht* heeft het HvJEU gevraagd of artikel 82 lid 1 AVG een specifiek of algemeen preventief karakter heeft, en of daarmee rekening gehouden moet worden bij de

---

175 HvJEU 4 april 2017, ECLI:EU:C:2017:256 (*Europese Ombudsman*), r.o. 91, 127 - 131. Zie ook: Gerecht EU 28 januari 1999, ECLI:EU:T:1999:11 (*BAI/Commisie)*, r.o. 38; HvJEU 9 november 2006, ECLI:EU:C:2006:708 (*Agraz e.a/Commissie*), r.o. 27; HvJEU 21 februari 2008, ECLI:EU:C:2008:107 (*Commissie/Girardot)i*, r.o. 54; Gerecht EU 10 januari 2017, ECLI:EU:T:2017:1 (*Gascogne/Europese Unie*), r.o. 145.

176 Gerecht EU 15 januari 2019, T-881/16, ECLI:EU:T:2019:5 (*HJ/EMA*).

177 HvJEU 6 februari 1986, C-173/82, C-157/83 en C-186/84, ECLI:EU:C:1986:54, (*Castille/Commissie*); HvJEU 17 december 1998, T-203/96, ECLI:EU:T:1998:302, paragraaf 108 (*Ambassade/Europees Parlement*); HvJEU 8 januari 1999, T-230/95, ECLI:EU:T:1999:11, paragraaf 39 (*BAI/Commissie*); HvJEU16 juli 2009, C-481/07, ECLI:EU:C:2009:461, paragraaf 38 (*SELEX Sistemi Integrati/Commissie*); Gerecht EU 10 Januari 2017, T577/14, ECLI:EU:T:2017:1, paragraaf 151 *(Gascogne/Europese Unie*).

178 Oberste Gerichtshof (Oostenrijk) 12 mei 2021, C-300/21 (*UI/Österreichische Post AG*).

179 Varhoven administrativen sad (Bulgarije) 14 mei 2021, C-340/21 (*VB/Natsionalna agentsia za prihodite*).

beoordeling van het immateriële schadebedrag. Ook vraagt deze rechter of de mate van schuld van de verwerkingsverantwoordelijke of verwerker een beslissende factor is bij de beoordeling van de hoogte van het immateriële schadebedrag.[180]

399. Het Duitse *Landgericht Saarbrücken* heeft vragen van gelijke strekking gesteld. Zo vraagt de Duitse rechter zich af of het begrip immateriële schade in artikel 82 AVG zo moet worden opgevat dat het elke aantasting van de beschermde rechtspositie omvat, ongeacht de overige gevolgen en de aanzienlijkheid ervan. Ook vraagt zij het HvJEU of het toelaatbaar of raadzaam is om de immateriële schade te baseren op de vaststellingscriteria van administratieve geldboeten uit artikel 83 AVG.[181]

400. De prejudiciële vragen die het Duitse *Amtsgericht Wesel* het HvJEU stelt, komen voor het grootste deel overeen met bovenstaande vragen. Relevant voor onderhavige zaak is de vraag of voor het ontstaan van een recht op vergoeding van immateriële schade voldoende is dat de eiser vreest dat ten gevolge van inbreuken op de bepalingen van de AVG zijn persoonsgegevens in vreemde handen zijn geraakt, zonder dat dit concreet kan worden vastgesteld.[182]

5.2.1.5 Conclusie A-G in UI/ Österreichische Post AG

401. Op 6 oktober 2022 heeft A-G Campos Sánchez-Bordona zijn conclusie genomen in bovengenoemde zaak betreffende Österreichische Post.[183] Österreichische Post verzamelde sinds 2017 informatie over partijaffiniteiten van de Oostenrijkse bevolking. Volgens bepaalde sociaal-demografische kenmerken had zij met behulp van een algoritme “adressen van doelgroepen” gedefinieerd ten behoeve van politieke reclame. UI is een natuurlijk persoon die onderwerp is geweest van deze gegevensverwerking. Hij had daarvoor geen toestemming gegeven. UI maakte zich boos over de gegevensverwerking en bovendien achtte hij de hem toegeschreven politieke affiniteit beledigend en schadelijk voor zijn reputatie. UI vorderde een immateriële schadevergoeding van € 1.000,-. In eerste aanleg werd de vordering afgewezen. In hoger beroep is dat vonnis bekrachtigd, waarbij de rechter overwoog dat niet iedere AVG-inbreuk automatisch recht geeft op immateriële schadevergoeding.

402. Tegen de uitspraak in hoger beroep is beroep in *Revision* (cassatie) ingesteld bij het Oberste Gerichtshof. Het Oberste Gerichtshof heeft in dat kader de volgende vragen gesteld aan het HvJEU:

a) Vereist de toekenning van schadevergoeding overeenkomstig artikel 82 AVG naast een inbreuk op de bepalingen van de AVG ook dat de eisende partij schade heeft geleden, of

[180] Bundesarbeitsgericht (Duitsland) 8 november 2021, C-66721 (*ZQ/Medizinischer Dienst der Krankenversicherung Nordrhein*).
[181] Landgericht Saarbrücken (Duitsland) 22 november 2021, C-741/21 (*GP/Juris GmbH*).
[182] Amtsgericht Wesel (Duitsland) 9 september 2022, C-590/22 (*PS*).
[183] Opinie A-G, zaak C-300/21 (*UI v Österreichische Post AG*).

volstaat reeds de inbreuk op bepalingen van de AVG als zodanig voor de toekenning van schadevergoeding?

b) Bestaan er voor de berekening van de schadevergoeding naast de beginselen van doeltreffendheid en gelijkwaardigheid andere Unierechtelijke bepalingen?

c) Is de opvatting dat de toekenning van immateriële schade veronderstelt dat er sprake is van een effect of gevolg van de schending dat op zijn minst van enig belang is en verder gaat dan de door de inbreuk ontstane ergernis, verenigbaar met het Unierecht?

403. De eerste prejudiciële vraag wordt door de A-G ontkennend beantwoord.

404. Ten eerste concludeert de A-G dat er geen recht op schadevergoeding bestaat als de Betrokkene geen schade heeft geleden door de inbreuk op de AVG.[184] Dat verbaast niet en is in lijn met hoe de Nederlandse rechtspraak omgaat met (immateriële) schadevergoeding. In het EBI-arrest (paragraaf 5.2.2.1) overwoog de Hoge Raad dat de enkele schending van een fundamenteel recht onvoldoende is om "aantasting op andere wijze in de persoon" aan te nemen.

405. Ten tweede concludeert de A-G dat de AVG niet voorziet in de mogelijkheid van punitieve schadevergoedingen en dat de factoren die in artikel 83 AVG worden genoemd voor het vaststellen van een op te leggen administratieve geldboete niet één-op-één kunnen worden overgenomen voor de begroting van de omvang van immateriële schade.[185] Sommige factoren zullen echter wel relevant zijn in het kader van de wettelijke aansprakelijkheid, zoals de opzettelijke of nalatige aard van de inbreuk.[186] Ook deze conclusies lijken geen invloed te hebben op de wijze waarop Nederlandse rechters omgaan met schadevergoedingen voor AVG-inbreuken of voor de beoordeling van de schadevordering in deze zaak. Stichting ICAM vordert geen punitieve schadevergoeding, maar vergoeding van daadwerkelijke en reële schade.

406. Ten derde gaat de A-G in op het concept van een "onbetwistbaar vermoeden van schade", waarvan de eiser lijkt te hebben betoogd dat daarvan sprake is zodra een inbreuk op de AVG heeft plaatsgevonden. Volgens eiser brengt een inbreuk noodzakelijkerwijs een verlies van controle over gegevens met zich mee, wat op zich schade zou opleveren die in aanmerking komt voor vergoeding.[187] Die uitleg acht de A-G onjuist.

407. De A-G overweegt dat in overwegingen 75 en 85 bij de AVG wordt verwezen naar controle over persoonsgegevens, maar dat in geen van beide overwegingen staat dat een inbreuk per se schade oplevert die in aanmerking komt voor vergoeding. Verlies van controle wordt genoemd als een gevolg dat kan voortvloeien uit een inbreuk in verband met persoonsgegevens,[188] maar dat hoeft

[184] Randnummers 27-34 van de Conclusie A-G.
[185] Randnummer 48 van de Conclusie A-G.
[186] Voetnoot 31 van de Conclusie A-G.
[187] Randnummers 56-57 van de Conclusie A-G.
[188] Randnummer 61 van de Conclusie A-G.

volgens de A-G niet onvermijdelijk tot schade te leiden. Emotionele gevolgen in verband met verlies van controle, zoals angst en bezorgdheid, resulteren uit het verlies, maar zijn er niet identiek aan.[189]

408. De A-G gaat vervolgens in op de vraag of controle over persoonsgegevens door een Betrokkene een waarde op zich is uit hoofde van de AVG. De automatische gelijkstelling tussen een verwerking zonder toestemming en schade die voor vergoeding in aanmerking komt, zou dat volgends de A-G veronderstellen.[190] De A-G is echter van mening dat controle "toezicht" betekent, en niet zozeer "macht" of "zeggenschap". De AVG verleent de Betrokkene het recht om toezicht uit te oefenen op en in te grijpen in activiteiten die anderen met betrekking tot de gegevens uitvoeren.[191] Dit lijkt in lijn met de ruime uitleg van het begrip zoals hierboven omschreven (paragraaf 5.2.1.1).

409. Uit de AVG kan volgens de A-G niet zomaar worden afgeleid dat het de bedoeling is de Betrokkene de controle over zijn persoonsgegevens te verlenen als een waarde op zich en evenmin dat de Betrokkene de grootst mogelijke controle over zijn gegevens dient te hebben.[192] De A-G overweegt dat wanneer de Betrokkene niet instemt met een verwerking en de verwerking bovendien zonder andere rechtmatige grondslag wordt uitgevoerd, dat nog niet betekent dat hij compensatie moet ontvangen wegens het verlies van controle over zijn gegevens. Verlies van controle levert op zichzelf geen schade op die voor vergoeding in aanmerking komt. Of in een concreet geval werkelijk schade is geleden, zal moeten worden bewezen.[193] Wel kan het verlies van controle volgens de A-G als leidraad dienen voor de vaststelling van immateriële schade, in die zin dat rekening wordt gehouden met hoe er wordt gereageerd ten aanzien van dat verlies.[194]

410. Ten aanzien van die reactie op het verlies van controle is nog relevant dat de A-G- overweegt dat het feit dat emoties of gevoelens niet onder woorden kunnen worden gebracht, vooral wanneer zij betrekking hebben op risico's omtrent wat er in de toekomst met de gegevens zou kunnen gebeuren, ertoe leidt dat zij niet als schade worden beschouwd omdat zij niet concreet genoeg zijn of een hypothetisch karakter hebben.[195] Daarvan is in de onderhavige zaak geen sprake, voor zover dat relevant is.

411. Indien het HvJEU de conclusies van de A-G volledig zou volgen, staat dat mogelijk op gespannen voet met de EBI-formule, waarin door de Hoge Raad wordt overwogen dat de aard en de ernst van de normschending mee kunnen brengen 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. Dit zou gezien kunnen worden als een (onweerlegbaar) vermoeden van

189 Voetnoot 43 van de Conclusie A-G.
190 Randnummer 68 van de Conclusie A-G.
191 Randnummer 71 van de Conclusie A-G.
192 Randnummer 74 van de Conclusie A-G.
193 Randnummer 77 van de Conclusie A-G.
194 Voetnoot 57 van de Conclusie A-G.
195 Voetnoot 69 van de Conclusie A-G.

schade, welke figuur door de A-G van de hand lijkt te worden gewezen. Aan de andere kant sluit de conclusie van de A-G niet expliciet uit dat in sommige gevallen wel een dergelijk vermoeden kan bestaan, gelet op de context van de schending (aard en ernst). In zulke gevallen wordt immers niet slechts volstaan met de conclusie dat sprake is van een schending en daarmee van schade, maar wordt ook acht geslagen op de specifieke omstandigheden van de schending.

412. Bij beantwoording van de tweede prejudiciële vraag overweegt de A-G dat het gelijkwaardigheidsbeginsel en het doeltreffendheidsbeginsel geen relevante rol spelen en dat bij de inhoudelijke invulling van schadevergoeding de AVG geen richtsnoeren biedt, waarbij wordt opgemerkt dat de schadevergoeding en de inhoudelijke invulling hiervan afhangt van de vordering die wordt ingesteld door de eisende partij.[196]

413. De derde prejudiciële vraag betreft de vraag of lidstaten een benedengrens mogen hanteren met betrekking tot de reactie van de benadeelde Betrokkene, in die zin dat hij geen schadevergoeding ontvangt als die reactie deze de-minimisdrempel) niet overschrijdt. De A-G beantwoordt deze vraag bevestigend.

414. De A-G schetst dat in overweging 75 van de AVG ongewenste gevolgen van elke verwerking worden vermeld en dat daarbij nadruk wordt gelegd (“met name”) op sommige gevolgen, hoogstwaarschijnlijk omdat die zwaarwegender zijn.[197] Het is volgens de A-G een beginsel van Unierecht dat immateriële schade wordt vergoed, waaruit echter niet kan worden afgeleid dat *alle* immateriële schade, ongeacht de ernst ervan, in aanmerking komt voor vergoeding.[198] Immateriële schade, mits die schade is bewezen, maakt deel uit van de werkelijk geleden schade, zo overweegt de A-G. Logischerwijs veronderstelt “bewijs” dat de schade reëel is, hetgeen het concept betreffende de ernst van de inbreuk benadert, maar er niet mee samenvalt. Niet duidelijk is waar de A-G met dat laatste precies op doelt, in de Engelse vertaling van de conclusie staat “seriousness of the damage”.[199]

415. Recht op schadevergoeding lijkt volgens de A-G niet het passende instrument om tegen inbreuken op te treden indien deze alleen maar boosheid of ergernis opwekken.[200] Bovendien wordt geen schadevergoeding toegekend voor zwakke en voorbijgaande gevoelens of emoties.[201] Daarvan is in onderhavige zaak geen sprake. Door het GGD-datalek bestaat bij Gedupeerden een concrete en reële angst. Er zijn immers gegevens gestolen en deze zijn verhandeld in het criminele circuit. Dit betekent dat er geen sprake is van loutere zwakke of voorbijgaande gevoelens.

196 Randnummers 83, 83 en 85 van de Conclusie A-G.
197 Randnummer 99 van de Conclusie A-G.
198 Randnummer 105 van de Conclusie A-G.
199 Voetnoot 79 van de Conclusie A-G.
200 Randnummers 113-114 van de Conclusie A-G
201 Randnummer 115 van de Conclusie A-G

416. Primair is Stichting ICAM van mening dat de overwegingen van de A-G over de gevolgen van een verlies van controle onjuist zijn. Controle over persoonsgegevens – in de ruime betekenis - is een centrale doelstelling van de AVG en wel degelijk een waarde op zichzelf. Zonder die controle kan de Betrokkene immers geen van zijn rechten op grond van de AVG uitoefenen, waarmee hij zijn rechten de facto verliest. Daarmee is het bestaan van schade gegeven. Subsidiair is Stichting ICAM van mening dat, ook indien verlies van control niet reeds op zichzelf schade meebrengt, daarvan in de onderhavige zaak wel sprake is. De A-G geeft aan dat het verlies van controle kan dienen als leidraad voor de vaststelling van immateriële schade, in die zin dat rekening wordt gehouden met hoe er wordt gereageerd ten aanzien van dat verlies. In dit geval zijn het (subsidiair) de gevolgen van het verlies van controle die kwalificeren als immateriële schade: verhoogde kwetsbaarheid voor criminaliteit, discriminatie, stigmatisering en de psychische gevolgen van het datalek (paragraaf 5.3.1). De A-G overweegt ook dat in overweging 75 bepaalde gevolgen worden benadrukt (“met name”), omdat die hoogstwaarschijnlijk zwaarwegender zijn. Dat kan betekenen dat als aannemelijk is dat dergelijke gevolgen voortvloeien uit een datalek, ook sneller immateriële schade aangenomen kan worden. De gevolgen die Stichting ICAM aanhaalt ten aanzien van het GGD-datalek, worden benadrukt in overweging 75.

5.2.2 Subsidiair: persoonlijke aantasting moet worden aangenomen wegens ernst van de overtreding

417. In Nederland is het recht op immateriële schadevergoeding neergelegd in artikel 6:106 lid 1 sub b BW. Dit artikel bepaalt dat een benadeelde recht heeft op vergoeding van immateriële schade indien hij lichamelijk letsel of een aantasting van eer of goede naam heeft geleden of "op andere wijze in zijn persoon is aangetast". De wetgever onderstreept in de parlementaire geschiedenis bij artikel 6:106 BW dat een inbreuk op de persoonlijke levenssfeer onder deze laatste categorie kan vallen. Eerbiediging van de persoonlijke levenssfeer omvat ook het recht om zelf te beslissen over de vergaring, het opslaan en het verstrekken van privé-gegevens (informationele privacy). Een inbreuk op de informationele privacy kan dan ook de toekenning van immateriële schadevergoeding rechtvaardigen.[202]

418. De persoonlijke aantasting "op andere wijze" kan verder worden onderverdeeld in twee categorieën. Ten eerste de categorie waarbij sprake is van aantoonbaar geestelijk letsel. Ten tweede de categorie waarbij sprake is van persoonlijk nadeel op andere wijze, waarbij geen sprake is van aantoonbaar geestelijk letsel.

419. Inbreuken op de AVG zullen vaak betrekking hebben op de tweede categorie, zo ook, subsidiair, in de onderhavige zaak (paragraaf 5.3).

[202] S.D. Lindenbergh, *Smartengeld*, Deventer: Wolters Kluwer 1998, p. 162-163.

5.2.2.1 Hoge Raad

420. Op 15 maart 2019 wees de Hoge Raad het *EBI*-arrest, waarin hij een kader schetst voor het recht op immateriële schadevergoeding bij het ontbreken van aantoonbaar lichamelijk of geestelijk letsel.[203] De hoofdregel is dat eiser met "concrete gegevens" moet kunnen aantonen dat hij in zijn persoon is benadeeld. In sommige gevallen kunnen de nadelige gevolgen van onrechtmatig handelen gelet op de aard en de ernst van de normschending echter zo duidelijk zijn dat persoonlijke aantasting mag worden aangenomen, zo oordeelde de Hoge Raad:

> "Van de in art. 6:106 lid 1, onder b, BW bedoelde aantasting in zijn persoon op andere wijze is in ieder geval sprake indien de benadeelde geestelijk letsel heeft opgelopen. Degene die zich hierop beroept, zal voldoende concrete gegevens moeten aanvoeren waaruit kan volgen dat in verband met de omstandigheden van het geval psychische schade is ontstaan, waartoe nodig is dat naar objectieve maatstaven het bestaan van geestelijk letsel kan worden vastgesteld (vgl. HR 23 januari 1998, ECLI:NL:HR:1998:ZC2551, rov. 3.4).
> Daarnaast kunnen de aard en de ernst van de normschending en van de gevolgen daarvan voor de benadeelde, meebrengen dat van de in art. 6:106 lid 1, onder b, BW bedoelde aantasting in zijn persoon op andere wijze sprake is (vgl. Parl. Gesch. Boek 6, p. 379 en p. 380). HR 29 juni 2012, ECLI:NL:HR:2012:BW1519 (Blauw oog) moet ook aldus worden verstaan.
> In beginsel zal degene die zich hierop beroept de aantasting in zijn persoon met concrete gegevens moeten onderbouwen. In voorkomend geval kunnen 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." [204]

421. Eiser hoeft dan niet aan te tonen dat hij daadwerkelijke nadelige gevolgen heeft ondervonden. Aangenomen wordt dat de Hoge Raad met het *EBI-arrest* de drempel voor het toekennen van immateriële schadevergoeding voor persoonlijke aantasting "op andere wijze", verlaagd heeft.

5.2.2.2 ABRvS

422. Op 1 april 2020 heeft de ABRvS vier uitspraken gewezen met betrekking tot immateriële schadevergoeding wegens AVG-inbreuken.[205] Alle vier de uitspraken van de ABRvS volgen de maatstaf zoals aangelegd door de Hoge Raad in het *EBI*-arrest.

423. Twee van deze zaken zijn vrijwel identiek. Eisers in die procedures hadden bij twee gemeenten een Wob-verzoek ingediend. Beide gemeenten hebben de NAW-gegevens van eisers vervolgens op het online forum van de Vereniging van Nederlandse Gemeentes ("**VNG**") geplaatst. Dat online forum wordt gebruikt om misbruik van de mogelijkheid tot het doen van een Wob-verzoek tegen te gaan, nu die mogelijkheid soms slechts voor het innen van dwangsommen wordt

[203] HR 15 maart 2019, ECLI:NL:HR:2019:376 (X/*EBI*).
[204] HR 15 maart 2019, ECLI:NL:HR:2019:376 (*X/EBI*), r.o. 4.2.1.
[205] ABRvS 1 april 2020, ECLI:NL:RVS:2020:900 (*X/Borsele*); ABRvS 1 april 2020, ECLI:NL:RVS:2020:901 (*X/Harderwijk*); ABRvS 1 april 2020, ECLI:NL:RVS:2020:899 (*Deventer/X*) ; ABRvS 1 April 2020, ECLI:NL:RVS:2020:898 (*Pieter Baan Centrum*).

gebruikt. Volgens eisers was de verwerking van hun gegevens op het forum onrechtmatig. Bovendien hebben eisers niet tijdig een overzicht van de hen betreffende, op het forum gedeelde, gegevens ontvangen. De ABRvS achtte het delen van de gegevens op het forum niet onrechtmatig, nu die verwerking ten doel heeft om de goede uitvoering van de Wob te verzekeren en misbruik te voorkomen. Het feit dat eisers niet tijdig een overzicht van hun persoonsgegevens op het VNG-forum was verstrekt, achtte de ABRvS wel onrechtmatig. De ABRvS overwoog echter dat zich in deze zaken geen situatie voordeed waarbij de nadelige gevolgen voor de hand liggen en persoonsaantasting kan worden aangenomen. De ABRvS wees de vordering tot immateriële schadevergoeding dan ook in beide zaken af.[206]

424. In de derde zaak werd ook geen immateriële schadevergoeding toegekend. In deze zaak had de gemeente Deventer de naam en het adres van eiser per e-mail medegedeeld aan een andere gemeente. Daarbij vermeldde de gemeente Deventer dat eiser twee Wob-verzoeken had ingediend. De rechtbank had in eerste aanleg al geoordeeld dat deze doorzending onrechtmatig was. De ABRvS overwoog echter dat de nadelige gevolgen van de normschending niet voor de hand liggen. Eiser had de aantasting in zijn persoon dan ook aannemelijk moeten maken, en de door hem gestelde schade met concrete gegevens moeten onderbouwen. Het ging volgens de ABRvS niet om ernstig verwijtbaar gedrag met zo ernstige gevolgen, dat dit als een inbreuk op een fundamenteel recht moest worden gekwalificeerd. Wel overwoog de ABRvS dat “verlies van controle” over persoonsgegevens kan worden aangemerkt als een aantasting van een persoonlijkheidsrecht.[207]

425. De ABRvS heeft in één van de uitspraken van 1 april 2020 wel immateriële schade toegekend, omdat het ging om een onrechtmatige verstrekking van bijzondere persoonsgegevens. De betrokkene hoefde de nadelige gevolgen van die verstrekking niet aan te tonen. Een directeur van het Pieter Baan Centrum had in een tuchtprocedure die door de eiser tegen hem was aangespannen medische gegevens van de eiser gedeeld met de tuchtrechter. In deze zaak werd bij het vaststellen van de hoogte van de schadevergoeding meegewogen dat het ging om bijzondere persoonsgegevens, maar dat de gegevens slechts bij een kleine groep professionals terecht waren gekomen. De ABRvS heeft uiteindelijk een schadevergoeding van € 500,- toegekend, hoger dan de vergoeding van € 300 zoals toegekend in eerste aanleg.[208]

426. Uit deze uitspraak is af te leiden dat bij de onrechtmatige verwerking van bijzondere persoonsgegevens aanleiding bestaat om immateriële schade te veronderstellen, gelet op de privacygevoeligheid van die gegevens. De drempel voor het aannemen van immateriële schade waar het gaat om onrechtmatige verwerking van bijzondere persoonsgegevens zonder dat

[206] ABRvS 1 april 2020, ECLI:NL:RVS:2020:900 (*X/Borsele*); ABRvS 1 april 2020, ECLI:NL:RVS:2020:901 (*X/Harderwijk*).
[207] ABRvS 1 april 2020, ECLI:NL:RVS:2020:899 (*Deventer/X*).
[208] ABRvS 1 April 2020, ECLI:NL:RVS:2020:898 (*Pieter Baan Centrum*).

sprake is van aantoonbaar geestelijk letsel,[209] is hiermee dan ook laag, dit in lijn met de rechtspraak van het HvJEU.

5.2.2.3 Lagere rechtspraak

427. In een zaak tussen een Betrokkene en het Uitvoeringsinstituut Werknemersverzekeringen ("**UWV**") oordeelde de rechtbank Amsterdam dat sprake was van verlies van controle over persoonsgegevens. Het UWV had informatie over een eerdere ziekte aan de nieuwe werkgever van de eiseres verstrekt, zonder dat daarvoor een wettelijke grondslag bestond. De rechtbank overwoog dat eiseres was getroffen in belangen die de AVG juist beoogt te beschermen. Het enkele feit dat de schade relatief gering (maar wel reëel) is, kan geen grond vormen om elke aanspraak daarop af te wijzen. De rechtbank oordeelde dat een AVG-conforme interpretatie van artikel 6:106 lid 1 BW meebracht dat eiseres recht had op vergoeding van haar schade en wees een bedrag van € 250,- toe.[210]

428. In een zaak tussen een journalist en een verhuurder over wie de journalist een kritisch artikel had geschreven, vorderde de journalist in reconventie schadevergoeding omdat de verhuurder een uittreksel uit de Gemeentelijke Basisadministratie had verstrekt aan twee partijen die geen recht hadden op ontvangst daarvan. Het uittreksel bevatte alleen de naam en het adres van de eiser. De eiser gaf aan nadelige gevolgen te hebben ondervonden, maar onderbouwde deze gevolgen niet. Toch achtte de rechtbank het met toepassing van het *EBI*-arrest aannemelijk dat eiser nadelige gevolgen, zoals angst en stress, had ondervonden als gevolg van het delen van zijn persoonsgegevens. Bovendien was het verlies van controle van eiser over zijn persoonsgegevens blijvend, zij het dat het verlies van controle beperkt was tot twee personen. Een schadevergoeding van € 250,- werd in dit geval passend en billijk geacht.[211]

429. In een zaak tussen een Betrokkene en de gemeente Oldambt had de gemeente per abuis de naam, het adres, het telefoonnummer, het e-mailadres en het BSN van de eiser op haar website gepubliceerd in plaats van alleen zijn naam en adres, hetgeen vereist was voor de bekendmaking van een besluit tot verlening van een milieuvergunning. De gegevens werden door de gemeente binnen vijf dagen verwijderd. De rechtbank oordeelde dat er sprake was van een schending van de AVG en dat de gemeente als gevolg daarvan aansprakelijk was voor de schade. Onder verwijzing naar het *EBI*-arrest kwam de rechtbank tot het oordeel dat de nadelige gevolgen voor de hand lagen. Zo stond de rechtbank onder meer expliciet stil bij het risico op identiteitsfraude als gevolg van het publiceren van de gegevens. De rechtbank kende een bedrag van € 500,- euro

---

209 T.F. Walree, *Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens,* (O&R nr. 126), diss. Nijmegen, Deventer: Wolters Kluwer 2021, p. 152. Zo betoogt ook AP-voorzitter Aleid Wolfsen: A. Wolfsen, 'Smartengeld moet de regel zijn, geen uitzondering', *Privacyblog Aleid Wolfsen* op www.autoriteitpersoonsgegevens.nl, 22 februari 2021 (**productie E.5**).

210 Rechtbank Amsterdam 2 september 2019, ECLI:NL:RBAMS:2019:6490 (X/UWV), r.o. 18.

211 Rechtbank Noord-Nederland 15 Januari 2020, ECLI:NL:RBNNE:2020:247 (*X/Y*) r.o. 4.106-4.107.

toe, gelet op de aard, de duur, de frequentie en de ernst van de inbreuk. Daarbij overwoog zij nog dat niet is gebleken dat de datalekken tot concrete negatieve gevolgen hebben geleid.[212]

430. De rechtbank Rotterdam heeft zich in haar uitspraak van 12 juli 2021 ook gebogen over een vordering tot immateriële schadevergoeding wegens een AVG-inbreuk.[213] Verzoekster in de procedure had verweerster, het college van burgemeester en wethouders van Rotterdam, verzocht om medische gegevens uit haar dossier te verwijderen. Het college had dat verzoek afgewezen. Ook het verzoek van verzoekster om terug te komen van dit besluit wees zij af. Later heeft het college aan verzoekster medegedeeld dat laatstgenoemd besluit werd ingetrokken en de medische gegevens toch werden verwijderd. De rechtbank oordeelde dat het college de medische gegevens van verzoekster onrechtmatig had verwerkt. Daarmee was ook het recht op eerbiediging van de persoonlijke levenssfeer geschonden, wat kan worden aangemerkt als een aantasting in de persoon als bedoeld in artikel 6:106 lid 1, onder b BW. Verzoekster had dan ook recht op immateriële schadevergoeding. Voor het vaststellen van de hoogte van die schadevergoeding achtte de rechtbank relevant dat de gegevens privacygevoelig zijn en gedurende ongeveer tien jaar zijn bewaard, ondanks verschillende verzoeken tot vernietiging. De rechtbank achtte bovendien aannemelijk dat meerdere personen en/of instanties van de inhoud kennis hadden kunnen nemen zonder dat zij daartoe gerechtigd waren en dat verzoekster daardoor immateriële schade heeft geleden. De rechtbank kende een immateriële schadevergoeding van € 2.500,- toe.

431. In een tweetal uitspraken van 25 februari 2022 heeft de kantonrechter van de rechtbank Rotterdam een immateriële schadevergoeding van € 250,- toegekend wegens verlies van controle over persoonsgegevens.[214] Gedaagde in beide procedures voerde in Zevenhuizen een nieuwbouwproject uit. Belangstellenden konden zich via een website inschrijven als kandidaat-koper. Van die mogelijkheid hebben ongeveer 1.100 personen gebruik gemaakt, waaronder eiser en eiseres in de twee procedures. Gedaagde heeft op enig moment een e-mail verzonden aan alle personen die zich hadden ingeschreven voor het project. Bij die e-mail heeft gedaagde een onbeveiligd Excelbestand gevoegd met daarin de gegevens van alle ingeschreven personen. Naast gegevens zoals voor- en achternaam, geboortedatum en –plaats en adres, bevatte de Excellijst ook financiële gegevens zoals gewenste koopsom, maximaal te lenen bedrag, jaarinkomen en eigen middelen die de kandidaat-koper wil inbrengen. Een minuut later heeft gedaagde geprobeerd het e-mailbericht in te trekken. Gedaagde heeft diezelfde avond een e-mail gestuurd waarin aangegeven werd dat de e-mail niet in alle gevallen kon worden ingetrokken en dat alle ontvangers met klem verzocht werd de e-mail te verwijderen. Eiser en eiseres vorderden in een procedure immateriële schadevergoeding. De kantonrechter overwoog dat verlies van controle is aan te merken als schade die voor vergoeding in aanmerking komt. Ten aanzien van de omvang van de schadevergoeding overwoog de kantonrechter dat gedaagde een

[212] Rechtbank Noord-Nederland 12 januari 2021, ECLI:NL:RBNNE:2021:106 (*X/Oldambt*), r.o. 4.28.
[213] Rb Rotterdam 12 juli 2021, ECLI:NL:RBROT:2021:6822 (*X/Rotterdam)*.
[214] Rb Rotterdam 24 februari 2022, ECLI:NL:RBROT:2022:1420; Rb Rotterdam 24 februari 2022, ECLI:NL:RBROT:2022:1419.

grote hoeveelheid persoonsgegevens heeft rondgestuurd, waaronder gevoelige financiële gegevens. Dat brengt risico's voor de Betrokkenen met zich mee. Anderzijds woog mee dat de gegevens niet openbaar waren gemaakt aan een algemeen publiek, maar slechts aan een in omvang beperkte groep. Verder achtte de rechtbank van belang dat het ging om een menselijke fout en dat gedaagde direct schadebeperkend heeft gehandeld. Ook was van belang dat het niet ging om bijzondere persoonsgegevens. De rechtbank wees met inachtneming van het voorgaande in beide procedures een immateriële schadevergoeding van € 250,- toe.

432. In een uitspraak van 21 september 2022 heeft de rechtbank Zeeland-West-Brabant een immateriële schadevergoeding toegewezen van € 2.000,- wegens veelvuldige onrechtmatige inzage in het patiëntendossier van eiseres. Gedurende een periode van ongeveer vier jaar had een medewerkster van het Bravisziekenhuis de nieuwe partner van de ex-man van eiseres, een groot aantal keren onrechtmatig inzage genomen in het medisch dossier van eiseres. De rechtbank ging ervan uit dat de medewerkster vertrouwelijke informatie uit dat dossier had gedeeld met anderen, onder andere met de ex-man van eiseres. Hij schreef op zijn beurt een boek over de echtscheiding en echtscheidingsperikelen, in welk boek ook medische gegevens van eiseres waren opgenomen. Het boek is uitgegeven door de eenmanszaak van de ziekenhuismedewerkster. Eiseres stelde het Bravisziekenhuis aansprakelijk voor de door haar geleden schade, onder meer omdat Bravis ten aanzien van de controle van de logging van patiëntendossiers geen passende beveiligingsmaatregelen had getroffen. De rechtbank volgde eiseres in dat betoog. Ten aanzien van het vaststellen van de hoogte van de immateriële schadevergoeding overwoog de rechtbank als volgt:

> "4.46 De rechtbank overweegt dat deze zaak op zijn eigen merites dient te worden beoordeeld. In deze zaak zijn fundamentele rechten geschonden; er is immers sprake van een inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer van [eiseres] en op het recht op bescherming van persoonsgegevens. De rechtbank is van oordeel dat sprake is van een situatie waarin de nadelige gevolgen voor [eiseres] zo voor de hand liggen dat een aantasting in de persoon als bedoeld in artikel 6:106, onder b, BW kan worden aangenomen. De rechtbank acht hierbij het volgende van belang. Het gaat hier om een bijzondere categorie van persoonsgegevens, namelijk medische persoonsgegevens uit een patiëntendossier van een ziekenhuis. Deze gegevens zijn over een langdurige periode van vier jaar veelvuldig onrechtmatig ingezien en zijn gedurende deze periode ook onvoldoende beschermd. Daarnaast is er ook medische informatie gedeeld met derden en gepubliceerd in een boek. Dat [eiseres] hier nadelige gevolgen van ondervindt, in de vorm van bijvoorbeeld angstklachten en het verlies van controle en de vertrouwelijkheid van haar persoonsgegevens, ligt voor de hand.
> 4.47. De rechtbank betrekt in haar oordeel ook dat in deze zaak artikel 32 van de AVG is geschonden. In de AVG zijn uitgangspunten geformuleerd voor de beoordeling van de schending, de (materiële en immateriële) schade en het causaal verband daartussen. Daarbij is in paragraaf 146 van de considerans neergelegd dat het begrip "schade" ruim moet worden uitgelegd in het licht van de rechtspraak van het Hof van Justitie, op een wijze die ten volle recht doet aan de doelstellingen van de verordening. Uit de AVG volgt het belang van controle over persoonsgegevens en handhaving van de geschonden regel. Een verordening-conforme uitleg van 6:106 lid 1 BW brengt (ook) mee

dat [eiseres] recht heeft op een naar billijkheid vast te stellen vergoeding van haar immateriële schade."

433. De rechtbank achtte een bedrag van € 2.000,- aan immateriële schadevergoeding passend, te betalen door het Bravisziekenhuis.

5.2.2.4 Buitenlandse rechtspraak

434. Het grondwettelijke hof van Duitsland, het *Bundesverfassungsgericht*, heeft onderstreept dat – ook in *de-minimis* gevallen – het begrip "schade" ruim moet worden uitgelegd in het licht van de rechtspraak van het HvJEU en op een wijze die ten volle recht doet aan de doelstellingen van de AVG. Aanleiding was een uitspraak van het *Amtsgericht* Goslar waarin het *Amtsgericht* een vordering tot immateriële schadevergoeding had afgewezen.[215] In deze zaak had een advocaat een bedrag van € 500,- aan immateriële schadevergoeding gevorderd omdat hij zonder voorafgaande toestemming één reclame-e-mail had ontvangen. Het *Amtsgericht* oordeelde dat op grond van artikel 82 AVG geen sprake was van (immateriële) schade omdat het ging om slechts één ongevraagde reclame e-mail waaruit evident bleek dat het om reclame ging en omdat de Betrokkene daardoor slechts tijdelijk ongemak had ondervonden. Het *Bundesverfassungsgericht* overwoog dat het *Amtsgericht* de vordering niet had mogen afwijzen op grond van een eigen uitleg van het recht, welke uitlegging noch rechtstreeks uit de AVG volgt, noch in de literatuur wordt bepleit of door het HvJEU wordt gebruikt. Het *Amtsgericht* had niet zonder prejudiciële verwijzing mogen beslissen dat uit de verzending van één e-mail op grond van artikel 82 AVG geen schadevordering van de eiser bestond.[216]

435. In december 2021 heeft het Landgericht München een Betrokkene een immateriële schadevergoeding van € 2.500,- toegekend. Deze zaak speelde zich af tussen een financiële dienstverlener en een klant van deze dienstverlener (eiser), en zag op een beweerdelijk datalek bij een *service provider* van de dienstverlener. Verweerder stelde eiser ervan in kennis dat derden onrechtmatig toegang hadden verkregen tot een deel van de klantgegevens van eiser, waaronder zijn volledige naam, contactgegevens en een kopie van een identiteitsbewijs. Eiser heeft aangevoerd dat derden via een cyberaanval toegang hadden tot persoonsgegevens van klanten, waarbij deze gegevens gekopieerd werden en op het *dark web* te koop werden aangeboden. Eiser stelde nu permanent te worden blootgesteld aan het risico slachtoffer te worden van identiteitsdiefstal en andere frauduleuze activiteiten. Het Landgericht kende immateriële schadevergoeding toe, hoewel er geen bewijs was dat de gestolen gegevens van eiser daadwerkelijk werden gebruikt voor frauduleuze doeleinden. Daarbij paste het *Landgericht* een ruime uitleg toe van artikel 82 AVG, waarbij zij overwoog dat eiser immateriële schade had geleden nu de aanvaller toegang had gekregen tot uitgebreide en gevoelige gegevens over eiser.

[215] Amtsgerichts Goslar 27 september 2019, 28 C 7/19.
[216] Bundesverfassungsgericht 14 januari 2021, 1 BvR 2853119.

Het *Landgericht* oordeelde bovendien dat de dienstverlener alle toekomstige materiële schade die eiser lijdt als gevolg van de ongeoorloofde toegang moet vergoeden.[217]

5.2.3 Tussenconclusie: ernst van de schending, de aannemelijkheid van gevoelens van stress, onrust en onbehagen en relevante factoren

436. Uit de hierboven behandelde rechtspraak blijkt dat de ernst van een schending van de AVG met zich mee kan brengen dat de nadelige gevolgen daarvan zo voor de hand liggen dat een persoonlijke aantasting mag worden aangenomen. De Betrokkene hoeft dan niet met concrete gegevens aan te tonen dat daarvan sprake is. De ernst van de normschending is in onderhavige zaak zodanig dat persoonlijke aantasting mag worden aangenomen (zie ook paragraaf 5.2.2). De Staat c.s. hebben verwijtbaar verschillende fundamentele beginselen uit de AVG veronachtzaamd, terwijl zij bijzondere persoonsgegevens van miljoenen burgers verwerken in de GGD-systemen. Zoals hierna uiteengezet zal worden, geven Deelnemers van Stichting ICAM ook blijk van deze persoonsaantasting. Zo geven zij te kennen gevoelens van stress te ervaren ten gevolge van het GGD-datalek (paragraaf 5.3.1.3).

5.3 Immateriële schade geleden door Gedupeerden

437. In deze paragraaf wordt omschreven welke negatieve gevolgen en risico's het GGD-datalek voor alle Gedupeerden heeft en welke immateriële schade daaruit voortvloeit. Voor alle Gedupeerden geldt dat zij door het GGD-datalek de controle over hun persoonsgegevens zijn verloren en hun rechten niet meer kunnen uitoefenen (paragraaf 5.3.1). Zij hebben een verhoogde kwetsbaarheid voor bijvoorbeeld online criminaliteit en fraude, voor zover online criminaliteit of pogingen daartoe niet al plaatsvinden ten gevolge van het GGD-datalek (paragraaf 5.3.1.1). Vaststaat immers dat gegevens zijn gestolen om ze te verkopen aan internetcriminelen. Bovendien zijn Gedupeerden verhoogd kwetsbaar voor intimidatie, discriminatie, stigmatisering en uitsluiting (paragraaf 5.3.1.2). Het voorgaande leidt tot aantasting van de persoon, in de vorm van psychische gevolgen (paragraaf 5.3.1.3) zoals onzekerheid, angst, stress en onbehagen. Deze gevoelens zijn reëel en invoelbaar.

438. Vervolgens licht Stichting ICAM toe hoe de hoogte van de immateriële schade in deze zaak moet worden berekend (paragraaf 5.3.2).

[217] Landgericht München 9 december 2021, 31 O 16606/20.

5.3.1 Immateriële schade door verlies van controle

439. In overweging 75 bij de AVG licht de Europese wetgever toe dat inbreuken op de rechten van natuurlijke personen vanwege onrechtmatige gegevensverwerkingen kunnen resulteren in ernstige lichamelijke, materiële of immateriële schade:

> "met name waar de verwerking kan leiden tot discriminatie, diefstal of -fraude, financiële verliezen, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, […] wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen; […] bij de verwerking van genetische gegevens of gegevens over gezondheid […]; wanneer persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, worden verwerkt; of wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen." (onderstreping door advocaat)

440. Uit deze formulering kan worden afgeleid dat reeds de mogelijkheid van discriminatie, diefstal of fraude voldoende is om tot schade te kunnen leiden. Ook kan hieruit worden afgeleid dat verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens op zichzelf voldoende is om tot die schade te kunnen leiden, evengoed als dat geldt voor de verwerking van gegevens over de gezondheid of van gegevens van kwetsbare personen, zoals kinderen, of wanneer grote hoeveelheden gegevens worden verwerkt met gevolgen voor een groot aantal betrokkenen.

441. De controle die natuurlijke personen over hun persoonsgegevens dienen te hebben, vormt de kern van de AVG.[218] Het verlies van controle is namelijk op zichzelf reeds schadelijk voor Betrokkenen. De Betrokkenen weten immers niet wat er met hun persoonsgegevens is gebeurd en of deze wellicht in criminele handen zijn. Gedupeerden van een datalek hebben daardoor een verhoogde kwetsbaarheid om daadwerkelijk slachtoffer te worden van criminaliteit, intimidatie, discriminatie, stigmatisering en uitsluiting. Deze verhoogde kwetsbaarheid leidt vervolgens tot psychische schade, ook wanneer de Betrokkenen nog niet daadwerkelijk slachtoffer zijn geworden van deze nadelige gevolgen.

5.3.1.1 Verhoogde kwetsbaarheid voor online criminaliteit

442. Bij datalekken buitgemaakte (gevoelige) persoonsgegevens worden vaak gebruikt voor (pogingen tot) verschillende vormen van online criminaliteit.

443. Cybercriminaliteit kan zich uiten in talloze verschijningsvormen, de bekendste hiervan zijn *phishing*, DDoS-aanvallen, identiteitsfraude en bijvoorbeeld Whatsapp-fraude. Daarnaast valt te denken aan telefoontjes die een slachtoffer ontvangt, waarbij criminelen gelekte gegevens gebruiken en zich voordoen als bijvoorbeeld een overheidsinstantie om mensen te bewegen tot

[218] Overweging 7.

acties; veelal het overmaken van een geldsom. Wanneer gevoelige gegevens lekken zoals het BSN, NAW-gegevens, geboortedata en contactgegevens, kunnen de gevolgen variëren van het doen van aankopen op naam van het slachtoffer tot grootschalige gevolgen zoals bankrekeningen openen, kredieten afsluiten of het doen van zaken met de overheid.[219] Ook kan bijvoorbeeld door middel van de verhuisservice van PostNL en het aanvragen van een nieuwe DigiD op naam van het slachtoffer, een bankrekeningnummer bij de Belastingdienst worden gewijzigd.

444. De AP wees er in het kader van een datalek bij Transavia in 2019 op dat buitgemaakte persoonsgegevens door oplichters gebruikt kunnen worden voor onder meer identiteitsdiefstal of voor het afhandig maken van geld, bijvoorbeeld middels WhatsApp-fraude (**productie C.20**). Ook bij boekingssite Booking.com werden in 2018 gegevens gestolen. De AP legde uit dat ook als geen creditcardgegevens zouden zijn ingezien, de overige gegevens gebruikt kunnen worden voor oplichting. Oplichters kunnen zich bijvoorbeeld voordoen als hotelpersoneel en gedupeerden geld afhandig maken (**productie C.15**). Bovendien kunnen persoonsgegevens afkomstig uit verschillende datalekken met elkaar gecombineerd worden, waardoor voor gedupeerden nog grotere risico's kunnen ontstaan.

445. In 2021, het jaar waarin het GGD-datalek aan het licht kwam, zijn 2,5 miljoen Nederlanders slachtoffer geworden van online criminaliteit (**productie C.26**).

446. De persoonsgegevens die zijn buitgemaakt uit de GGD-systemen zijn nog aantrekkelijker voor online criminaliteit dan de gegevens afkomstig uit bovengenoemde datalekken. Ten eerste is in de GGD-systemen een uitgebreid scala aan (bijzondere) persoonsgegevens van Gedupeerden opgeslagen. De systemen bevatten onder meer naam, adres, woonplaats, telefoonnummer, e-mailadres, BSN, geslacht, geboortedatum, test- en/of vaccinatieafspraken en testresultaten, contra-indicaties en COVID-19 klachten. Ook wordt informatie uit BCO vastgelegd (**producties F.15 t/m F.18)**. Criminelen kunnen zich hiermee een indringend beeld vormen van de Gedupeerden en dat in hun voordeel gebruiken voor malafide praktijken. Ten tweede zijn de gegevens uit het GGD-datalek zeer betrouwbaar omdat deze van de overheid afkomstig zijn.

447. GGD GHOR erkent dat Gedupeerden van het GGD-datalek een risico lopen slachtoffer te worden van identiteitsfraude (**productie F.15 en F.21**). De belangrijkste identiteitsgegevens zoals naam, geboortedatum en BSN zijn immers gecompromitteerd. GGD GHOR wijst er in de brief aan de Gedupeerden ook op dat de persoonsgegevens uit het GGD-datalek gebruikt kunnen worden voor *phishing*. Gedupeerden kunnen nepe-mails en neptelefoontjes krijgen van criminelen die zich bijvoorbeeld voordoen als GGD-medewerker en hen op die manier (nadere) gegevens afhandig proberen te maken of proberen over te halen geld over te maken.

448. Zelfs inbraak en diefstal zijn potentiële gevolgen. Immers, door de geboortedatum in combinatie met adresgegevens en gezondheidsgegevens kunnen gemakkelijk adressen van kwetsbare

[219] Zie onder meer 'Soorten Identiteitsfraude', Rijksoverheid.nl, geraadpleegd op 2 december 2022.

ouderen gefilterd worden door inbrekers. Dit geldt ook voor bekende mensen, waarvan bekend is dat (adres-)gegevens te koop zijn aangeboden (paragraaf 3.1.1).

449. Dat online criminaliteit ten gevolge van het GGD-datalek niet illusoir is, blijkt uit een bericht van de Fraudehelpdesk. Reeds enkele dagen na bekendwording van het GGD-datalek meldde de Fraudehelpdesk dat zij al ongeveer veertig eerder door haar ontvangen meldingen kon koppelen aan het GGD-datalek (**productie C.12**).

450. Stichting ICAM heeft bovendien van meerdere Gedupeerden berichten ontvangen dat zij *phishing* e-mails hebben ontvangen. Een aantal Deelnemers ontving een e-mail die eruitzag alsof deze van de GGD afkomstig was. Daarin stonden in veel gevallen persoonlijke gegevens en werden zij uitgenodigd voor een boosterprik. Voor de aanmelding werden bankgegevens opgevraagd (**productie K.8 t/m K.10**). Veel Deelnemers verklaren dat zij meer *phishing* e-mails en brieven hebben ontvangen sinds het GGD-datalek en dat zij vermoeden dat dit wordt veroorzaakt door het datalek. Zij ontvangen onder andere nepe-mails als afkomstig van de Belastingdienst, verzekeraars, incassobureaus, Post NL, Waternet en Woningnet (producties **K.13 t/m K.17**).

451. Ook werd een Deelnemer enige tijd nadat hij zich had laten testen door de GGD gebeld door iemand die daarvan op de hoogte was. Vervolgens werden zijn gegevens opgevraagd, maar een oplettende vriendin die op dat moment aanwezig was nam de telefoon over en kapte het gesprek af (**productie K.11**). Weer een andere Deelnemer ontving nadat zij een positieve uitslag had gekregen, een drietal WhatsApp berichten van onbekende personen (**productie K.12**). Ook andere Deelnemers zijn telefonisch benaderd, regelmatig vanuit het buitenland. In sommige gevallen leek het erop dat telefoonnummers van Deelnemers gebruikt werden als doorschakelnummer, om met dat nummer weer andere mensen te bellen (**productie K.16 en K.18)**. Verder zijn er situaties bekend waarin mensen telefonisch werden bedreigd of onder druk gezet (**productie K.19**). Zo deden de criminelen zich voor als de politie of het Amerikaanse openbaar ministerie, benaderden ze mensen mobiel of op het werk en beschikten ze over allerlei gevoelige persoonsgegevens (**productie K.20**).

452. Ook uit verschillende Woo-stukken blijkt dat de risico's op online criminaliteit ten gevolge van het GGD-datalek niet theoretisch zijn, maar zich daadwerkelijk hebben verwezenlijkt:

a) In een agenda van de Projectgroep Covid-19 van de GGD Noord- en Oost Gelderland d.d. 21 februari 2021 wordt opgemerkt: "Het lijkt erop dat er naar aanleiding van de datadiefstal 'vreemde' dingen zien [sic.] in de teststraten. Voorbeeld: mensen die getest worden, krijgen in de loop van de dag een bericht dat zou opnieuw getest moeten worden en zich moeten melden in onze teststraten (het lijkt dan dat het bericht vanuit de GGD komt, wat niet zo is). We hebben deze mensen niet gebeld en ook de uitslag is op dat moment nog helemaal niet bekend." (**productie G.51**);

b) Uit een actieplan Informatiebeveiliging van de GGD Noord- en Oost-Gelderland blijkt dat er in oktober 2021 *phishing* acties plaatsvonden (**productie G.45**, p. 1) (uit dit actieplan blijkt overigens dat deze GGD op een veelheid verschillende onderwerpen de AVG-compliance nog niet op orde had in 2021, waaronder op het vlak van controle van loggingoverzichten (p. 4));

c) Uit een weekverhaal van de GGD Rotterdam-Rijnmond blijkt dat van 85 burgers gegevens zijn gebruikt om hen telefonisch te benaderen met het verzoek om te betalen voor een afgenomen coronatest (**productie G.59**, p. 22). Daarnaast volgt uit het weekrapport dat niet duidelijk is hoeveel claims er bij de GGD Rotterdam-Rijnmond zijn ingediend.

5.3.1.2 Verhoogde kwetsbaarheid voor intimidatie, discriminatie, stigmatisering en uitsluiting

453. Wanneer persoonsgegevens eenmaal vrij circuleren op het internet zijn de potentiële gevolgen moeilijk uitputtend te beschrijven. Online criminaliteit zal voor een belangrijk deel gericht zijn op het verkrijgen van financieel gewin. Het naar buiten komen van bepaalde gevoelige persoonsgegevens kan echter ook op andere gebieden negatieve gevolgen hebben. Zo kan het openbaar worden van gegevens negatieve gevolgen hebben voor iemand arbeidspositie of leiden tot hogere premies bij een verzekeringsaanvraag. Dit is met name denkbaar wanneer medische gegevens worden gelekt, zoals bij het GGD-datalek.

454. In de literatuur worden daarnaast andere potentiële gevolgen van datalekken beschreven zoals *doxing* (het gebruik van persoonsgegevens om iemand te intimideren) en stalking. Zoals in paragraaf 3.1.1 reeds aan de orde is gekomen, is bekend dat de persoonsgegevens van bekende mensen waaronder de Rotterdamse burgemeester Aboutaleb ongeoorloofd zijn ingezien en dat door medewerkers telefoonnummers zijn uitgewisseld van mensen die zich hadden laten testen.

455. Dat de angst voor enige vorm van intimidatie, discriminatie, stigmatisering en uitsluiting niet denkbeeldig is, en dat de gegevens uit het GGD-datalek niet enkel gebruikt werden voor online fraude van een abstracte groep mensen, volgt wel uit de verklaringen van verbalisanten die onderzoek deden naar het GGD-datalek (**productie J.3**). Hieruit blijkt dat zelfs de contactgegevens van een zestienjarig meisje werden verhandeld en dat het zoeken op een specifiek persoon bij de verkoop van de gegevens als mogelijkheid werd aangeprezen:

> "Ik zag dat er meerdere gesprekken via WhatsApp gevoerd werden met [H]. […] Ik zag dat [verdachte] op 18 november 2020 een foto deelde met [H] van een 25 jarige vrouw, waarbij besproken werd dat het de zus van een bekende was en dat ze positief getest was. Ik zag dat er op 14 december 2020 een foto gedeeld werd via Whatsapp door ' [verdachte] ' met ' [H] ' waarop het CoronIT systeem zichtbaar was met de gegevens van een 21 jarige vrouw zichtbaar waren. Ik zag dat voorafgaand aan deze foto het bericht 'Ik heb een cadeautje voor je' gestuurd werd. Ik zag dat [verdachte] op 17 januari 2021 een foto deelde met [H] waarop de gegevens te zien waren van een zestien jarig meisje."

> "Ik zag dat het volgende bericht […] geplaatst was in diverse Telegram groepen door gebruiker Meneer [gebruikersnaam 1] […]: !! !! Ben je opzoek naar iemand zijn adres, BSN-nummer etc. Dan ben je hier aan het juiste adres. Bericht me voor meer info !! !!
> Ik zag dat het account ' [instagram account] ' op 27 december 2020 via Instagram de volgende twee berichten stuurde aan gebruiker ' [gebruikersnaam 6] ':
> Hey, ik kan iedereen zijn adres, bsn nummer etc. Fixen
> en
> Wellicht kan je hier gebruik van maken en hebben we beiden wat aan elkaar"

456. Dat ook daadwerkelijk mensen zijn benaderd volgt ook uit de verklaring van de verbalisanten:

> "Tevens zag ik een gesprek met [gebruikersnaam 4] waarbij gebruiker [I] haar informeert dat haar gegevens opgevraagd zijn bij hem door ' [gebruikersnaam 3] ."

457. Het behoeft weinig toelichting dat niet alleen bekende Nederlanders en jonge vrouwen potentieel het slachtoffer zijn van intimidatie als gevolg van gebrekkige beveiliging van de GGD-systemen. Afhankelijk van de specifieke kwaadwillende motieven van de koper van de gegevens, kan het datalek iedereen treffen. In dit kader speelt ook nog een rol de gevoeligheid van gegevens die te maken hebben met het al dan niet volgen van het coronabeleid van de overheid in sociale zin. Uit KPMG-privacyonderzoek van 2021 blijkt dat 31% van de Nederlanders de keuze om wel of niet te vaccineren tegen corona voor zichzelf wenst te houden. Voor de Gedupeerden van het GGD-datalek bestaat de mogelijkheid om informatie over het volgen van het coronabeleid of een besmetting met het coronavirus, voor henzelf te houden, niet meer. Deze informatie kan op elk moment weer opduiken.

5.3.1.3 Psychische gevolgen van verhoogde kwetsbaarheid

458. Al in 1890 signaleerden Samuel Warren en Louis Brandeis het risico dat technologie tot mentale en emotionele schade kan leiden in hun artikel "*The Right to Privacy": "modern enterprise and invention have, through invasions upon his privacy, subjected [man] to mental pain and distress, far greater than could be inflicted by mere bodily injury*."[220]

459. Uit onderzoek van het Europees Bureau voor de Grondrechten (*the European Union Agency for Fundamental Rights*) in 2013 onder rechtzoekende gedupeerden in zestien representatieve lidstaten – waaronder Nederland - blijkt dat de schade die betrokkenen lijden naar aanleiding van een inbreuk op het gegevensbeschermingsrecht met name wordt geleden in psychische zin (zoals door stress of angst) of sociale zin (de mening van anderen of impact op hun relaties met andere mensen).[221] Het relevante hoofdstuk van het onderzoek worden overgelegd als **productie E.1**.

---

[220] S. Warren & L. Brandeis, 'The Right to Privacy', *Harvard Law Review*, 4-5. (1890), p. 196.

[221] *European Union Agency for Fundamental Rights,* Access to Data Protection Remedies in EU Member States (Publication Office of the European Union 2013), p. 28.

460. De respondenten gaven aan verschillende vormen van schendingen te hebben ervaren. De meest voorkomende waren gelegen in onrechtmatige gegevensverwerkingen, waaronder door excessieve verwerking en opslag van gegevens door publieke autoriteiten zonder adequate beveiligingsmaatregelen, opslag van onnodig veel gegevens en de ongeoorloofde openbaarmaking van gegevens aan ongeautoriseerde personen. Publieke autoriteiten en private entiteiten gingen gelijk op in de schending van het recht op gegevensbescherming. Organisaties in de gezondheidszorg worden in het onderzoek specifiek genoemd als risico.[222]

461. De respondenten noemden verschillende vormen van emotionele nood, belediging, onveiligheid (waaronder het gevoel onder surveillance te staan), hulpeloosheid of reputatieschade, gebrek aan vertrouwen en andere vormen van immateriële of "morele" schade. Een respondent in Spanje noemde specifiek het gevoel van "onmacht ten aanzien van machtsmisbruik".[223]

462. Uit het onderzoek blijkt dat financiële schade zelden een reden was om naar de rechter te stappen. In de gevallen waarin financiële schade was opgetreden, werd dit door de Betrokkenen als minder belangwekkend ervaren dan de emotionele gevolgen. Daadwerkelijk misbruik van gelekte gegevens, zoals identiteitsfraude, was bovendien niet noodzakelijk om schadelijke gevolgen te ervaren. Een respondent zei hierover:

> "'Simply the uncertainty – not knowing, even who has this data, and how it's been used – is the damage. There might be other more particular damages but I don't know about them. And of course that's why access is so important. Why accounting for the use and disclosure of information is so important. Without that, one cannot know what other problems there may be, or what damage may have been done.' (Complainant, France) "[224]

463. KPMG onderzoekt sinds de invoering van de AVG in 2018 jaarlijks hoe Nederlanders over hun privacy denken. Uit het privacyonderzoek van 2021 komt naar voren dat zorgen over privacy sinds 2018 substantieel zijn toegenomen (**productie K.2**). Nederlanders zijn bezorgd over datalekken. Bijna twee derde (63%) is bang dat hierdoor persoonlijke gegevens op straat komen te liggen. 86% van de Nederlanders maakt zich zorgen over *phishing*.

464. De psychologische gevolgen van datalekken worden ook steeds uitgebreider onderzocht vanuit verschillende wetenschappelijke disciplines, met name in de Verenigde Staten en het Verenigd Koninkrijk.

465. Uit psychologisch onderzoek van de Universiteit van Cambridge in 2015 blijkt dat in gevallen waarin daadwerkelijk sprake was van online fraude, respondenten te kennen gaven de

[222] Ibid., p. 26.
[223] Ibid., p. 28.
[224] *Ibid.*

emotionele gevolgen aanmerkelijk ernstiger te beoordelen dan de financiële gevolgen, om welke vorm van online fraude het ook ging:[225]

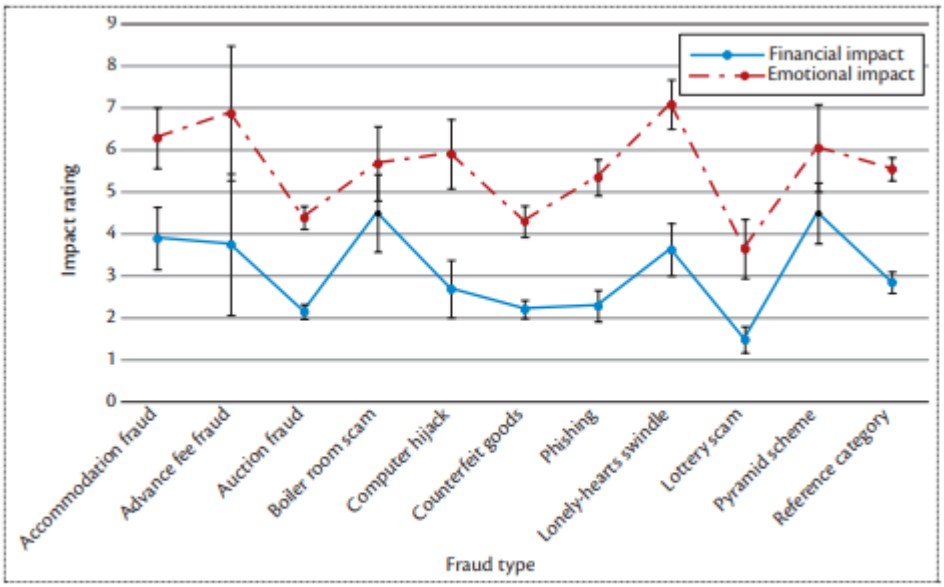


Figure 1. The participants' average reported impact for each fraud category. Boiler room fraud had the highest reported financial loss, closely followed by pyramid schemes and accommodation fraud.

466. Professor Recht & Psychologie aan de Universiteit van Birmingham Hugh Koch concludeert in 2019 dat betrokkenen psychologisch en sociaal zwaar kunnen worden getroffen door datalekken. Typische psychologische effecten zijn gevoelens van slachtofferschap, van streek zijn en depressieve gevoelens, slapeloosheid, eet- en slaapproblemen en sociale angst. In een significant aantal gevallen waarin psychologische effecten na een datalek werden vastgesteld, kwam de mate van verstoring en ontwrichting overeen met erkende psychologische stoornissen zoals aanpassingsstoornissen, depressieve stoornissen, angststoornissen en in extreme gevallen zelfs posttraumatische stressstoornissen (**productie E.2**).[226]

467. Amerikaans onderzoek uit 2020 laat zien dat 86% van de getroffen betrokkenen gevoelens van bezorgdheid, woede en frustratie ervoer, 70% het gevoel had dat zij anderen niet meer konden vertrouwen en zich onveilig voelde, meer dan 66% gevoelens van machteloosheid en hulpeloosheid ervoer en 59% zelfs verdriet en depressie. Deze emoties kunnen vervolgens ook psychologische gevolgen hebben. 85% van de getroffen betrokkenen rapporteerde

[225] D. Modic & R. Anderson, 'It's All but the Crying: The Emotional and Financial Impact of Internet Fraud', in: *Ieee Security & Privacy*, 13-5, p. 102.
[226] H. Koch and N. Adeleye, 'Psychological Injury, Cyber Crime and Data Breach Damages', *The Expert Witness Journal* 26 (2019), p. 53-55.

slaapstoornissen, 77% toegenomen stress, 64% concentratieproblemen en in 57% van de gevallen werden pijnen en krampen gemeld (**productie E.3**).[227]

468. In een artikel uit 2021 van Kilovaty, Associate Professor of Law aan de Universiteit van Tulsa en Visiting Faculty Fellow en Affiliated Fellow aan Yale Law School, wordt verwezen naar wetenschappelijk onderzoek waarin wordt benadrukt dat de blootstelling van persoonsgegevens door een datalek kan leiden tot angst, depressie, posttraumatische stress en paranoia bij de Betrokkenen van wie de gegevens zijn gecompromitteerd. Ook geeft hij aan dat onderzoek heeft laten zien dat de Betrokkenen de emotionele impact vaak als erger ervaren dan de financiële gevolgen. Betrokkenen hebben gerapporteerd dat een datalek waarin gevoelige gegevens zijn gecompromitteerd, "*left them feeling dizzy with shock*". Wetenschappelijk onderzoek heeft zelfs de prevalentie van diagnosticeerbare psychische stoornissen als gevolg van datalekken bevestigd, zoals depressieve stoornissen, paniekstoornissen en pleinvrees. Ander onderzoek vergelijkt deze psychologische effecten van datalekken met die van trauma-overlevers en slachtoffers van inbraak en mishandeling (**productie E.4**).[228]

469. Kilovaty maakt een onderscheid tussen subjectieve en objectieve schade ten gevolge van dataleken.[229] Subjectieve schade wordt gedefinieerd als de "*perceptie van ongewenste observatie*", hetgeen bij een datalek een gegeven is. Betrokkenen wiens informatie in het verleden is gecompromitteerd, kunnen allerlei emoties voelen en allerlei psychische aandoeningen ervaren. De auteur duidt dit soort subjectieve schade als een centraal onderdeel van psychologische schade door datalekken en acht het van cruciaal belang dat psychologische schade als subjectief wordt aangemerkt. Deze categorisering weerspiegelt de belangrijke gedachte dat de getroffen Betrokkenen psychische schade als gevolg van een datalek kunnen ondervinden zonder dat sprake hoeft te zijn van daadwerkelijk misbruik van de gegevens. Veel van de beschreven subjectieve schade is ook objectief, inhoudende dat ze een "nadelig, reëel gevolg" hebben. Objectieve schade van inbreuken op gegevens zijn "extern aan het slachtoffer", in die zin dat de schade een externe actie inhoudt met betrekking tot de informatie die is gecompromitteerd. Zo kunnen kwaadwillenden de gegevens gebruiken voor oplichting of identiteitsfraude. De auteur geeft aan dat het verband tussen subjectieve en objectieve schade door datalekken wellicht niet vanzelfsprekend is, maar dat objectieve schade wel de factor is die de subjectieve schade die Betrokkenen bij een datalek kunnen ondervinden - verhoogde angst, depressie, angst, PTSS en andere aandoeningen - versterkt.

470. Verklaringen van de Gedupeerden van het GGD-datalek laten een beeld zien dat overeenkomt met het onderzoek dat hierboven is aangehaald:

---

[227] J. Guynn, Anxiety, 'Depression and PTSD: The Hidden Epidemic of Data Breaches and Cyber Crimes', in: USA Today 24 februari 2020.
[228] Ido Kilovaty, 'Psychological Data Breach Harms', in: *North Carolina Journal of Law & Technology*, 23-1, article 2 (2021), p. 18 en 19.
[229] Ibid., p. 42-44.

"(…) Helaas ben ik een van de gedupeerden die een brief van de GGD ontving op 7 juni 2021. Ik was zó verbaasd dat dit in deze organisatie kon gebeuren. Sinds die tijd ben ik heel alert op alles wat ik aanklik, betaal etc. geen leuke manier van leven. Altijd wantrouwen.
Dat heb ik ook met uw actie, ik bedoel maar… dit is een gok wat ik nu doe. Mijn vinger heeft een lange tijd boven de enter toets gehangen om te durven klikken. Site/voorwaarden steeds maar weer doorlezen.
Zo ziet u, hoe mijn leven hierdoor is veranderd. Ik heb steeds het idee dat ze ergens op de 'loer' liggen. Zowel fysiek (adresgegevens) als via internet/telefoon etc." (**productie K.7**)

"(Waarschijnlijk) vorig jaar heeft hij zich laten testen aan de Koploperstraat in Utrecht. Grote GGDtestlocatie. Ik kan niet meer precies nagaan wanneer exact, maar het was ieg in het begin van de tijd van de testlocaties.
Kort daarna werd hij gebeld door een dame. "Met [achternaam]." "Dag meneer [achternaam], u heeft zich kort geleden laten testen op corona. Mogen wij uw gegevens even checken? Uw adres is ……." En [voornaam] noemde zijn adres. Ik hoorde het gesprek even aan en gebaarde mij de telefoon te geven, want ik rook lont. Ze probeerde verder te gaan met mij, maar ze strandde al vlug." (**productie K.11**)

"Goeden avond, ik zag jullie actie tegen de GGD dataleak en ik ben zo blij mee. Dit jaar heb ik zo veeel oplichters die mij proberen te bestelen. ik bleef mijzelf afvragen, hoe komen deze mensen aan mijn gegevens!? Ik had deze mobiel nummer meer dan 10 JAAR. ik word nu steeds gebeld door apart nummers en raar emails krijg ik om dingen te betalen met apart linkje. ik ben op conclusie gekomen dat mijn gegegevens zijn geleaked via ggd want Ik gaf nooit mijn number naar ander mensen en ik heb best een kleine kring om mijn heen. Ik vind dit zo hinderlijk, zeker nu wanr ik probeer te solliciteren maar ik weet niet wie de oplichters zijn en wie mij belt voor werk, ik wacht af tot ik een voicemail heb om te weten als ik mensen kan terug bellen. Ik ben jullie heel erg dankbaar voor jullie aktie. Het hoort niet zo te gaan,goei voorbeeld van de oplichters zie je bij de bijlage, zeker wanneer ik geen bankpas had aangevraagd of een pakket verwacht.
Nou, ik wou even mijn verhaal delen, heel erg bedankt," (**productie K.13**)

"Ik heb mij aangemeld voor de claim, maar ik wil er nog wat over kwijt. Ik weet dat er uitzendkrachten en personen uit de bijstand het telefonische afspraak werk deden voor de GGD. Dit deden zij vanuit huis op hun eigen computer of laptop. Daar had ik al mijn vraagtekens bij. Toen ik een afspraak wilde maken voor mijn eerste vaccinatie moest ik aan een wildvreemd persoon mijn BSN nummer doorgeven. Dit wilde ik niet omdat dit mijn persoonlijke nummer is en ik niet wist wie ik aan de andere kant van de lijn aan de telefoon had. De medewerker liet mij weten dat ik dan geen afspraak kon maken. Daarop heb ik aangegeven dat ik mijn BSN nummer op het vaccinatie station wilde laten zien, maar dat ik niet wilde dat het ergens genoteerd werd. Dit was niet mogelijk. Om veilig en zonder risico door de maatschappij te kunnen bewegen heb ik toen toch mijn bSN nummer doorgegeven. Sindsdien wordt ik via de post, mail en telefonisch lastig gevallen met SPAM .Ik krijg brieven van de belastingdienst, verzekeringen, incasso bureaus, betalingen voor postNL en appjes of ik geld kan overmaken. Ik ben dan nu gevaccineerd maar voel mij niet meer veilig in deze SPAM wereld, ieder moment van de dag ben ik bang dat mijn bankrekening geplunderd wordt omdat ik per ongeluk en in mijn goede vertrouwen toch ergens op een SPAM bericht gereageerd heb." (**productie K.15**)

> "Hallo, kan het ook zijn dat ik lastig gevallen word door telefoon nummers uit binnen en buitenland??
> En bij opnemen word mijn telefoon gekraakt en met mijn nummer weer andere mensen lastig gevallen?? Dit is ook sedert de vaccinatie aan de gang, neem geen onbekend nummer meer op" (**productie K.18**)

> "Ik steun jullie initiatief maar wil niet al mijn persoonlijke gegevens zomaar online zetten. Ik ben getest door de GGD en heb daar schade van ondervonden. Wij wonen in Heiloo in een veilige en nette buurt en regelmatig ontving ik telefoontjes van criminele organisaties die geld wilde hebben en dreigende taal uitspraken. Nu weet ik dat een medewerker van de GGD in Heiloo persoonlijke gegevens heeft doorgespeeld van patiënten. De dreigingen zijn vanzelf opgehouden totdat ik hun nummer heb geblokkeerd. Jullie actie is heel goed omdat ik mij heel erg alleen voelde en aangifte doen bij de politie heeft toch weinig zin." (**productie K.19**)

471. Ook de Staat c.s. zijn zich bewust van de psychische gevolgen die een ernstig datalek als het GGD-datalek kan hebben voor Betrokkenen. Zo is in een brief van de DPG van de GGD Noord- en oost Gelderland aan het algemeen bestuur van die GGD te lezen:

> "We ervaren bij mensen die zich hebben laten testen, vaccineren en hebben meegedaan aan bron- en contactonderzoek emoties als verontwaardiging, verdriet en frustratie. Bezorgdheid en boosheid. Ongeloof en onbegrip. Het spijt ons dat dit zo heeft kunnen gebeuren. Wij begrijpen heel goed dat mensen van wie de gegevens in onze systemen zitten ongerust zijn en vragen hebben." (**productie G.50**)

472. Dat het GGD-datalek tot veel zorgen onder de Gedupeerden heeft geleid blijkt ook uit het feit dat de AP na het GGD-datalek zelfs enige tijd slecht bereikbaar was omdat een zeer groot aantal mensen ongerust contact met haar zocht (**productie C.7**).

473. Het GGD-datalek leidt ook tot de situatie dat Gedupeerden voor zover mogelijk de controle over hun persoonsgegevens proberen terug te krijgen, ondanks dat zij de reële kans moeten accepteren dat de gegevens al in verkeerde handen zijn beland en de controle dus voor altijd verloren is. Dit blijkt onder andere uit mailverkeer bij de GGD Rotterdam-Rijnmond, waar sinds het GGD-datalek in korte tijd ruim 300 AVG-verwijderingsverzoeken werden ingediend door boze en verontwaardigde burgers.

474. De psychologische gevolgen van het GGD-datalek ontstaan bij alle Gedupeerden en zijn onomkeerbaar. Dit maakt ook dat de gevolgen niet zomaar eindigden toen de Staat c.s. eindelijk maatregelen troffen. Vooral voor de groep Gedupeerden waarvan niet kan worden vastgesteld of er gegevens zijn ontvreemd zullen de psychische gevolgen van verhoogde kwetsbaarheid lang aanhouden. Zij ervaren immers stress en andere psychische gevolgen zoals hierboven besproken door de onwetendheid over wat er met hun gegevens is gebeurd.

5.3.1.4 Tussenconclusie: Gedupeerden ondervinden immateriële schade die voor vergoeding in aanmerking komt

475. Uit het bovenstaande volgt dat de Gedupeerden door het GGD-datalek immateriële schade lijden. Het datalek heeft verlies van controle over de bijzondere persoonsgegevens van Gedupeerden tot gevolg. Uit overweging 75 bij de AVG blijkt dat een dergelijk verlies van controle met name in gevallen zoals de onderhavige leidt tot ernstige schade, nu het gaat om de verwerking van gezondheidsgegevens en een grote hoeveelheid andere data van een groot aantal Betrokkenen. Het GGD-datalek leidt niet alleen tot verhoogde kwetsbaarheid van Gedupeerden voor online criminaliteit, maar ook voor intimidatie, discriminatie, stigmatisering en uitsluiting, zulks gelet op de buitgemaakte gegevens (onder meer achterliggende medische aandoeningen en vaccinatiestatus). Deze verhoogde kwetsbaarheid heeft invoelbare en reële psychische gevolgen voor Gedupeerden. Zo ervaren Gedupeerden onder meer een grote mate van onzekerheid, angst, en stress.

476. Deze immateriële schade komt, gelet op het eerder geschetste toetsingskader voor immateriële schadevergoedingsvorderingen, primair voor vergoeding in aanmerking op grond van de AVG en subsidiair op grond van het Nederlandse schadevergoedingsrecht.

5.3.2 Berekening van de omvang van immateriële schade

477. Stichting ICAM vordert in onderhavige procedure vanwege de immateriële schade forfaitaire bedragen van respectievelijk € 500,- voor iedere Gedupeerde die deel uitmaakt van Gedupeerden Categorie A en € 1.500,- voor iedere Gedupeerde die deel uitmaakt van Gedupeerden Categorie B (paragraaf 9.1.3.1).

5.3.2.1 Forfaitaire schadeberekening

478. Het Nederlandse recht biedt de mogelijkheid om op deze abstracte wijze immateriële schadevergoeding te begroten. Artikel 6:97 BW bepaalt immers dat de rechter de schade zal begroten op de wijze die het meest met de aard ervan in overeenstemming is en dat de rechter de schade mag schatten, wanneer deze niet nauwkeurig kan worden vastgesteld. Artikel 6:97 BW biedt dus een wettelijke grondslag voor het (al dan niet geschat) op abstracte wijze begroten van schadevergoeding.

479. Bij abstracte schadebegroting houdt de rechter in een of meer opzichten niet zozeer rekening met de bijzonderheden van het desbetreffende geval en met de subjectieve omstandigheden waarin de benadeelde zich bevindt, maar gaat hij na hoe groot in het algemeen de schade is van een schuldeiser die in een gelijksoortige positie verkeert als de eiser in het geding.[230]

[230] C.H. Sieburgh, '35. Abstracte wijze van vaststelling schade.' in: *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel II. De verbintenis uit de wet*., Deventer: Wolters Kluwer 2021.

Aanknopingspunten voor een abstracte benadering kunnen aldus gevonden worden in de aard van de schade, eisen van doelmatigheid en in de redelijkheid van het resultaat.[231]

480. Voor zover nodig dient artikel 6:97 BW AVG-conform te worden uitgelegd, om zo recht te doen aan de doelstellingen van de AVG en het ruime schadebegrip daarin.

481. In (de aard van) de WAMCA ligt besloten dat een zekere mate van abstrahering doorgaans ook logisch zal zijn. Indien voor iedere benadeelde op individueel niveau moet worden onderzocht wat de concrete schade is, zou de WAMCA geen meerwaarde hebben ten opzichte van individuele procedures. Het is voor individuele eisers niet economisch om een procedure te beginnen voor een te laag schadebedrag. Een WAMCA-procedure dient hierbij dan ook een publiek belang. Voor een efficiënte en effectieve massaschaderegeling is het onvermijdelijk om te abstraheren van individuele omstandigheden.[232] Bij de invoering van de WAMCA is dan ook expliciet gewezen op deze wijze van schadebegroting.[233] Artikel 1018i lid 2 Rv biedt zelfs expliciet een wettelijke grondslag voor het begroten van schadevergoeding op forfaitaire basis. Dat artikellid bepaalt dat de rechter bij de vaststelling van de collectieve schadeafwikkeling de schadevergoeding "*waar mogelijk in categorieën vaststelt*", hetgeen in wezen neerkomt op forfaitering, en dat de toegekende schadevergoeding "*redelijk*" dient te zijn.[234]

482. De Hoge Raad heeft ook al geoordeeld dat begroting van immateriële schade op een forfaitair bedrag mogelijk is. Daartoe overwoog de Hoge Raad dat de rechter aannemelijk kan achten dat de door de persoonsaantasting geleden schade ten minste een bepaald bedrag beloopt, indien de nadelige gevolgen evident zijn gelet op de aard en de ernst van de gebeurtenis waarop de aansprakelijkheid berust.[235]

483. In wezen wordt in de Nederlandse rechtspraak over schadevergoedingen voor AVG-inbreuken ook telkens de omvang van de immateriële schade geschat dan wel abstract vastgesteld. De bedragen die door de ABRvS en lagere rechters zijn vastgesteld hebben een forfaitair karakter, en zijn niet gebaseerd op een concrete berekening van geleden schade (paragraaf 5.2.2.2 en 5.2.2.3).

484. Bij immateriële schade ten gevolge van AVG-inbreuken ligt de begroting van immateriële schade op forfaitaire bedragen bovendien voor de hand. Zo schrijft Lindenbergh in zijn noot bij het *EBI*-arrest:

---

231 S.D. Lindenbergh, *Schadevergoeding: algemeen, deel 1* (Monografieën BW B34), Deventer: Wolters Kluwer 2021, p. 53.
232 T. Hartlief, 'Massaschade en de regelende rechter', *Blog NJB,* 13 november 2017, te vinden via https://www.njb.nl/blogs/massaschade-en-de-regelende-rechter/.
233 *Kamerstukken II* 2016/17, 34 608, nr. 3, p. 5.
234 Zie ook *Kamerstukken II* 2016/17, 34 608, nr. 3, p. 52.
235 HR 19 juli 2019, ECLI:NL:HR:2019:1278 (*Aardbevingsschade Groningen*). Zie ook HR 26 oktober 2012, ECLI:NL:HR:2012:BX0357 (*Reaal Schadeverzekering/Athlon Car Lease*), r.o. 3.6.2 en 3.7.

> "Bij — kort gezegd — schending van fundamentele rechten ligt het evenwel veel meer voor de hand om de omvang van de vergoeding te relateren aan de aard en ernst van de normschending. Daarbij gaat het immers veeleer om veronderstelde gevolgen. Dat laat, afhankelijk van het type geval, ook vrij goed tarifering (categoriebedragen) van bedragen toe: bij massale inbreuk op de persoonlijke levenssfeer door een datalek van belangrijke privégegevens ligt het voor de hand om aan alle benadeelden eenzelfde bedrag toe te wijzen." [236]

485. Normering van schadevergoeding is bovendien wenselijk gelet op de bijdrage die met het schadevergoedingsrecht geleverd kan worden aan de effectieve handhaving van het gegevensbeschermingsrecht. Het is immers onaanvaardbaar dat een gedupeerde nooit aanspraak zou kunnen maken op schadevergoeding omdat de risico's die voortvloeien uit een AVG-inbreuk moeilijk objectiveerbaar en kwantificeerbaar zijn, zelfs al staat de inbreuk op de AVG vast. Daarmee zou de gedupeerde de risico's moeten dragen die de inbreukmaker in het leven heeft geroepen, terwijl de AVG de gedupeerde juist probeert te beschermen tegen die risico's.[237]

486. In onderhavige zaak is gelet op het bovenstaande een abstracte begroting van de omvang van de schadevergoeding op zijn plaats. De nadelige gevolgen van het onrechtmatig handelen door de Staat c.s. zijn evident, gelet op de aard en de ernst van het GGD-datalek. Grote hoeveelheden persoonsgegevens, waaronder bijzondere persoonsgegevens, zijn buiten de controle van de Gedupeerden geraakt doordat zij toegankelijk waren voor alle GGD-medewerkers, zijn gestolen en online te koop zijn aangeboden. De overtreding is des te ernstiger omdat de Staat c.s. fundamentele beginselen van de AVG hebben geschonden. Bovendien gaat het in onderhavige zaak om schendingen door de overheid, aan wie burgers nu juist bij uitstek hun persoonsgegevens zouden moeten kunnen toevertrouwen. Het is dan ook aannemelijk dat de geleden schade ten minste een bepaald bedrag dient te belopen.[238] Stichting ICAM vordert om die reden dan ook toewijzing van een forfaitaire schadevergoeding per Gedupeerde.

5.3.2.2 Factoren voor het begroten van immateriële schade

487. Bij het bepalen van de hoogte van immateriële schadevergoeding dient als uitgangspunt te worden genomen dat het recht op schadevergoeding een daadwerkelijke en doeltreffende rechtsbescherming moet waarborgen.[239] Daartoe dient – zoals hierboven geconcludeerd – gekeken te worden naar de aard en de ernst van de schending en de aannemelijkheid van gevoelens van stress, onrust en onbehagen ten gevolge van die schending (paragraaf 5.3). Om hieraan invulling te geven, kan gekeken worden naar de factoren die in de Nederlandse rechtspraak zijn toegepast bij het bepalen van de hoogte van immateriële schadevergoeding, en

---

[236] HR 15 maart 2019, ECLI:NL:HR:2019:376 (*X/EBI*), NJ 2019/162 met annotatie van S.D. Lindenbergh, par. 18.
[237] M.C. Samsom, 'Normering van schadevergoeding in gegevensbeschermingszaken', *AV&S* 2022/3, afl. 1.
[238] HR 19 juli 2019, ECLI:NL:HR:2019:1278 (*Aardbevingsschade Groningen*).
[239] HvJEU 10 april 1984, ECLI:EU:C:1984:153 (*Von Colson en Kamann*), r.o. 23 - 24; HvJEU 2 augustus 1993, ECLI:EU:C:1993:335 (*Marshall*), r.o. 24; HvJEU 22 april 1997, ECLI:EU:C:1997:208 (*Draehmpaehl*), r.o. 25; HvJEU 17 december 2015, ECLI:EU:C:2015:831 (*Camacho*), r.o. 31.

naar artikel 83 lid 2 AVG, dat factoren opsomt die kunnen worden toegepast bij het bepalen van de hoogte van administratieve boetes voor AVG-schendingen. Tezamen vormen deze factoren een goede omstandighedencatalogus:

a) De aard van de gegevens, zoals gevoelige of bijzondere persoonsgegevens;[240]

b) De aard en de ernst van de overtreding;[241]

c) De duur van de inbreuk en de genomen actie om de inbreuk ongedaan te maken;[242]

d) Het aantal betrokkenen;[243]

e) De onomkeerbaarheid van de schade;[244]

f) Het opzettelijke of nalatige karakter van de inbreuk;[245]

g) De door de verantwoordelijke genomen maatregelen om de schade te beperken;[246]

h) De mate waarin de verwerkingsverantwoordelijke verantwoordelijk is gezien de technische en organisatorische maatregelen die hij heeft uitgevoerd overeenkomstig artikelen 25 en 32 AVG (of heeft nagelaten uit te voeren);[247]

i) Eerdere relevante inbreuken;[248]

j) De mate waarin met de AP is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken;[249]

k) De wijze waarop de AP kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke de inbreuk heeft gemeld;[250] en

[240] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, r.o. 36; Artikel 83 lid 2 sub g AVG.
[241] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, r.o. 36; Artikel 83 lid 2 sub a AVG.
[242] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, r.o. 36; Rb. Rotterdam 12 juli 2021, ECLI:NL:RBROT:2021:6822, r.o. 4.3; Artikel 83 lid 2 sub a AVG
[243] Rb. Noord-Nederland 15 januari 2020, ECLI:NL:RBNNE:2020:247, r.o. 4.107; Artikel 83 lid 2 sub a AVG.
[244] Rb. Amsterdam 2 september 2019, ECLI:NL:RBAMS:2019:6490, r.o. 18; Rb. Noord-Nederland 15 januari 2020, ECLI:NL:RBNNE:2020:247, r.o. 4.107.
[245] Artikel 83 lid 2 sub b AVG.
[246] Artikel 83 lid 2 sub c AVG.
[247] Artikel 83 lid 2 sub d AVG.
[248] Artikel 83 lid 2 sub e AVG.
[249] Artikel 83 lid 2 sub f AVG.
[250] Artikel 83 lid 2 sub h AVG.

l) Elke andere verzwarende of verzachtende omstandigheid die op de omstandigheden van het geval van toepassing is;[251]

m) Categorie van de schending: schending van de belangrijkste beginselen van artikel 5 AVG worden beschouwd als ernstige schendingen, waarvoor dan ook hogere boetes kunnen worden opgelegd.[252]

5.3.2.3 Toepassing op de onderhavige zaak

488. Toetsing aan deze factoren leidt tot de conclusie dat de hoogte van de toe te kennen immateriële schade aan de bovenkant van de bandbreedte uit zou moeten komen zoals die kan worden afgeleid uit de Nederlandse rechtspraak. De algemene regel lijkt te zijn dat in het geval meerdere factoren wijzen op toekenning van schadevergoeding, een significant hoger bedrag aan schadevergoeding wordt toegewezen.

489. Een belangrijke factor bij het toekennen van een (hoge) schadevergoeding is blijkens de rechtspraak of er bijzondere of gevoelige persoonsgegevens betrokken zijn bij de inbreuk. Als dat het geval is, wordt doorgaans een hogere vergoeding toegekend. Daarnaast is de omvang van de groep personen relevant welke door het datalek de beschikking heeft gekregen over de persoonsgegevens van de Betrokkenen. Als het gaat om een groot aantal personen, wordt doorgaans een hoger bedrag toegewezen. Ook de duur van de inbreuk kan van invloed zijn op de hoogte van de toe te kennen schadevergoeding.

De aard van de gegevens

490. De GGD-systemen bevatten een grote hoeveelheid persoonsgegevens van de Gedupeerden, waaronder bijzondere persoonsgegevens in de zin van artikel 9 AVG. In de systemen werden immers gezondheidsgegevens geregistreerd (testuitslagen, coronagerelateerde klachten, gegevens om te beoordelen of iemand een vaccinatie kan krijgen en vaccinatie-afspraken). Daarnaast bevatten de systemen van de GGD ook gevoelige gegevens, zoals BSNs.

De aard en de ernst van de overtreding

491. De overtredingen van de AVG door de Staat c.s. zijn bijzonder ernstig. De Staat c.s. hebben nagelaten om zelfs maar de meest basale beveiligingsmaatregelen te treffen om bijzondere gegevens te beschermen van miljoenen mensen, terwijl zij al langere tijd bekend waren met de kwetsbaarheid van de systemen. De Gedupeerden lopen daardoor grote risico's. Niet alleen zijn de Gedupeerden de controle over hun (bijzondere) persoonsgegevens verloren, ook lopen zij het

[251] Artikel 83 lid 2 sub k AVG.
[252] Artikel 83 lid 4 AVG en Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2019).

risico om slachtoffer te worden van illegale praktijken zoals identiteitsfraude. Doordat de Staat c.s. hebben nagelaten adequate organisatorische en technische (beveiligings)maatregelen te nemen, schendt zij fundamentele beginselen van de AVG. Wat de overtredingen des te ernstiger maakt is dat het hier gaat om de overheid. Burgers zijn in grote mate overgeleverd aan gegevensverwerking door de overheid en moeten er dan ook op kunnen vertrouwen dat hun gegevens met de grootst mogelijke zorgvuldigheid worden behandeld. Dat blijkt niet het geval te zijn. Daarmee hebben de Staat c.s. het vertrouwen van burgers dan ook ernstig geschaad.

De duur van de inbreuk en de genomen actie om de inbreuk ongedaan te maken

492. De Staat c.s. schenden de AVG al sinds het moment dat de GGD-systemen in gebruik werden genomen voor de bestrijding van het coronavirus, in februari 2020. De Staat c.s. waren er op dat moment al van op de hoogte dat de GGD-systemen niet geschikt waren voor de verwerking van persoonsgegevens op deze grote schaal (**productie D.1B**). De Staat c.s. ontvingen bovendien in september 2020 al signalen dat onbevoegde GGD-medewerkers alle gegevens in de systemen in konden zien (**productie D.4**). Ook nadat zij kennisnamen van die signalen hebben de Staat c.s. geen (adequate) maatregelen genomen om de kwetsbaarheden in de GGD-systemen te verhelpen. De maatregelen die de Staat c.s. na het bekend worden van het datalek hebben genomen waren bovendien niet voldoende om de risico's voor betrokkenen weg te nemen, zo bevestigt de AP (**productie C.19**). De inbreuk duurt dan ook nog steeds voort.

Het aantal betrokkenen

493. Het gaat om een zeer groot aantal Betrokkenen, in totaal in ieder geval 6,5 miljoen mensen.

De onomkeerbaarheid van de schade

494. De Gedupeerden zijn de controle over hun persoonsgegevens kwijt. Zij verkeren dan ook in blijvende onzekerheid met betrekking tot de vraag of zij slachtoffer zullen worden van schadelijke en/of illegale praktijken. Zelfs als dat niet het geval is, blijft staan dat sprake is van persoonsaantasting nu onbevoegden toegang hebben (gehad) tot de bijzondere persoonsgegevens van Gedupeerden. Bovendien zijn en blijven de Gedupeerden verhoogd kwetsbaar voor dergelijke schadelijke en/of illegale praktijken als gevolg van het datalek.[253] De schade is dan ook onomkeerbaar.

Het opzettelijke of nalatige karakter van de inbreuk

495. De handelswijze van de Staat c.s. is zeer nalatig. De Staat c.s. waren ervan op de hoogte dat de systemen van de GGD niet geschikt waren om op deze grote en intensieve schaal ingezet te

[253] M.C. Samsom, 'Normering van schadevergoeding in gegevensbeschermingszaken', *AV&S* 2022/3, afl. 1.

worden (**producties C.5 en C.10** en randnummers 71, 80, 90, 208, 492). Bovendien werden zij meermaals gewaarschuwd dat de bescherming van persoonsgegevens binnen de systemen van de GGD niet op orde was (**productie C.8** en paragraaf 3.1). Toch hebben zij nagelaten adequate actie te ondernemen.

De door de verantwoordelijke genomen maatregelen om de schade te beperken

496. De Staat c.s. hebben enkele maatregelen genomen nadat het datalek bekend is geworden. Zo hebben zij de zoekfunctie in de systemen beperkt en het aantal personen dat gegevens uit de systemen kan exporteren teruggebracht. Die maatregelen zijn echter pas genomen toen het kwaad voor de Gedupeerden al was geschied. Immers, GGD-medewerkers konden vanaf het moment dat de GGD-systemen werden ingezet voor de bestrijding van het coronavirus alle gegevens inzien. Van deze maatregelen kan dan ook niet gezegd worden dat zij het risico voor de Gedupeerden hebben beperkt.

De mate waarin de verwerkingsverantwoordelijke verantwoordelijk is gezien (gebrek aan) technische en organisatorische maatregelen

497. De Staat c.s. hebben nagelaten adequate technische en organisatorische maatregelen te nemen om de persoonsgegevens van de Gedupeerden te beveiligen tegen ongeoorloofde inzage door GGD-medewerkers en diefstal van gegevens. Zelfs nadat zij signalen kreeg dat de GGD-systemen niet (voldoende) beveiligd waren, hebben de Staat c.s. daar niet adequaat op gereageerd. De Staat c.s. zijn dan ook volledig verantwoordelijk te houden voor het datalek uit de GGD-systemen en de schade die daaruit voor de Gedupeerden voortvloeit.

Eerdere relevante inbreuken

498. De Staat c.s. hebben – voor zover bekend - in deze samenstelling niet eerder inbreuk gemaakt op de AVG. Wel vinden binnen de overheid regelmatig datalekken en andere gegevensbeschermingsincidenten plaats.[254] De Staat c.s. kunnen zich daarom ook niet meer verschuilen achter een verontschuldiging en een toezegging het beter te gaan doen. Dit datalek is van ongekende omvang en mede gelet op het feit dat de AP heeft besloten niet te handhaven, is het van belang dat de Staat c.s. in deze procedure nu wel verantwoordelijk worden gehouden.

De mate waarin met de AP is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken

[254] De AP rapporteert jaarlijks over het aantal datalekken binnen verschillende sectoren: Autoriteit Persoonsgegevens, 'Overzichten datalekken', te raadplegen op: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken.

499. Stichting ICAM heeft geen concrete informatie over de mate waarin de Staat c.s. met de AP hebben samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen van de inbreuk te beperken.

De wijze waarop de AP kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke de inbreuk heeft gemeld

500. GGD GHOR heeft op 22 januari 2021, mede namens de GGD'en, melding gedaan van het datalek (**productie F.15**). Zoals uiteengezet in paragraaf 3.1 bestonden echter al veel eerder duidelijke aanwijzingen dat van een datalek sprake was. De Staat c.s. hadden daarvan dan ook al veel eerder melding moeten doen.

Verzwarende of verzachtende omstandigheden

501. Een verzwarende omstandigheid is dat burgers tijdens de coronapandemie feitelijk weinig keuze hadden ten aanzien van gegevensverwerking door de Staat c.s. Om het coronavirus zo goed mogelijk te bestrijden, hebben de Staat c.s. aldoor een beroep gedaan op de test- en vaccinatiebereidheid van burgers. Om daar uitvoering aan te geven is gegevensverwerking noodzakelijk, en de burger zou er dan ook van uit moeten kunnen gaan dat zorgvuldig met persoonsgegevens zou worden omgegaan. Gebleken is echter dat de Staat c.s. bijzonder nalatig hebben gehandeld.

502. De Staat c.s. zullen als verzachtende omstandigheid waarschijnlijk aanvoeren dat sprake was van een crisissituatie, de GGD-systemen in alle snelheid in gebruik moesten worden genomen en dat er geen tijd was om de nodige aanpassingen en maatregelen door te voeren. Dat argument gaat echter niet op. Zoals in de inleiding besproken, is het niet zo dat een omvangrijke infectieziekteuitbraak zoals de coronapandemie niet was voorzien. Lang voordat de eerste coronabesmetting plaatsvond begin 2020 wist men dat de dag zou komen dat er een grote epidemie of pandemie zou uitbreken en dat de verouderde GGD-systemen dan niet geschikt en veilig zouden zijn. Men had daar op voorbereid moeten zijn. In een crisissituatie zoals de coronapandemie is het immers veel moeilijker om zaken in de hand te houden, terwijl het belang van goede informatiebeveiliging dan juist exponentieel toeneemt. Bovendien hadden alle landen ter wereld te maken met dezelfde crisis en voor zover bekend is het nergens zo fout gegaan als in Nederland.

503. Echter, ook nadat de systemen in gebruik waren genomen voor de bestrijding van corona, zijn de Staat c.s. er meerdere malen op gewezen dat de gegevens van miljoenen mensen gevaar liepen. Ook toen namen zij nog steeds geen, althans onvoldoende stappen om de gebreken te herstellen. Zelfs als het zo zou zijn dat sprake was van een onvoorziene crisissituatie en dat die situatie rechtvaardigde dat beveiligingsnormen niet werden nageleefd, dan heeft dat argument een beperkte houdbaarheidsdatum. Op enig moment had naast de pandemiebestrijding ook de

beveiliging van de bijzondere persoonsgegevens van miljoenen mensen een prioriteit moeten worden.

Categorie van schendingen

504. De Staat c.s. hebben fundamentele beginselen van de AVG geschonden, zoals de plicht om persoonsgegevens adequaat te beveiligen, het beginsel van dataminimalisatie en de verantwoordingsplicht. Bovendien zien deze inbreuken op bijzondere persoonsgegevens, waar op grond van artikel 83 lid 5 AVG de hoogste boetes voor op kunnen worden gelegd.

505. Gelet op het bovenstaande zijn Stichting ICAM c.s. van mening dat de gevorderde forfaitaire immateriële schadevergoedingen van respectievelijk € 500,- voor iedere Gedupeerde die deel uitmaakt van Gedupeerde Categorie A en € 1.500,- voor iedere Gedupeerde die deel uitmaakt van Gedupeerden Categorie B, redelijk zijn. Deze vergoedingen zijn in lijn met eerder door Nederlandse rechters toegewezen schadevergoedingen.

5.4 Materiële schade geleden door de Gedupeerden

506. Het GGD-datalek heeft ook geleid tot materiële schade voor alle Gedupeerden. De tijd die door de Staat c.s. vooraf niet besteed is aan het adequaat beveiligen van gevoelige persoonsgegevens, zodat het GGD-datalek voorkomen had kunnen worden, komt nu voor rekening van de Gedupeerden, met de kanttekening dat het verlies van controle dat Gedupeerden hebben geleden, naar zijn aard blijvend is. Er is geen manier waarop Gedupeerden deze controle kunnen heroveren.

507. Het enige dat zij kunnen doen, is de mogelijke gevolgen enigszins verkleinen door hun e-mailadres en telefoonnummer bij alle instanties waar Gedupeerden contact mee hebben, te wijzigen. Dit is een enorm karwei, waar Gedupeerden langdurig tijd aan besteden. Ook zullen de Gedupeerden continu alert moeten zijn op mogelijke gevolgen. Het nalopen van bankafschriften en het volgen van de berichtgeving omtrent datalekken, kost tijd. Ook zullen de Gedupeerden tijd moeten besteden aan het beoordelen en controleren van bijvoorbeeld potentiële *phishing* e-mails en van accounts en bankrekeningen. Tijd die de Gedupeerden anders hadden kunnen besteden.

508. Stichting ICAM erkent dat uiteraard niet alle 6,5 miljoen Gedupeerden daadwerkelijk (evenveel) tijd zullen besteden aan mitigerende en controlerende maatregelen. Aannemelijk is echter wel dat een belangrijk deel van hen dat zal doen, getuige bijvoorbeeld de vele berichten die Stichting ICAM heeft ontvangen van haar Deelnemers. Ook het feit dat het GGD-datalek (terecht) zoveel aandacht heeft gekregen in de media zal daaraan bijdragen. Stichting ICAM is dan ook van mening dat het in deze zaak gerechtvaardigd is om ook de materiële schade vast te stellen op een zekere forfaitaire ondergrens.

509. De materiële schade die Gedupeerden lijden bestaat uit verloren tijd die zij moeten besteden aan de volgende maatregelen:

a) Het volgen van berichtgeving over het datalek en de buitgemaakte persoonsgegevens;

b) Het (extra) controleren van de betrouwbaarheid van ontvangen telefoontjes, e-mails, brieven en andere correspondentie, bijvoorbeeld door instanties na te bellen;

c) Het controleren van bankafschriften en accounts;

d) Het (al dan niet preventief) wijzigen van contactgegevens zoals telefoonnummers en e-mailadressen;

e) Het doorgeven van gewijzigde van contactgegevens bij instanties waar Gedupeerden contact mee hebben;

f) Het (al dan niet preventief) aanpassen van wachtwoorden en andere inloggegevens, bijvoorbeeld voor DigiD;

g) Het (al dan niet preventief) blokkeren van (betaal)rekeningen, bankpassen en creditcards;

h) Het inschakelen van monitoringsdiensten voor (verdachte) afschrijvingen op (betaal)rekeningen.

510. Het is moeilijk in te schatten hoeveel tijd Gedupeerden kwijt zijn aan het nemen van deze mitigerende maatregelen. Een grote groep Gedupeerden maakt zich enorme zorgen over het datalek en zal maandenlang dagelijks bankafschriften en correspondentie controleren. Een schatting van 30 minuten per week gedurende een periode van zes maanden is naar mening van Stichting ICAM al conservatief en zou leiden tot een tijdsinvestering van ongeveer 13 uur. Een ander deel van de Gedupeerden zal echter minder tijd besteden aan mitigerende maatregelen. Een tijdsinvestering van 2 uur aan mitigerende maatregelen in totaal is dan ook een zeer conservatieve schatting. Stichting ICAM is bereid om haar vordering voor alle Gedupeerden te baseren op deze conservatieve inschatting.

511. Voor wat betreft de vergoeding die voor ieder geïnvesteerd uur toegekend zou moeten worden, verwijst Stichting ICAM naar verschillende Amerikaanse schikkingen in zaken omtrent privacy-inbreuken.[255] In dergelijke zaken is een vergoeding van vijfentwintig dollar per uur gebruikelijk. Dat komt op het moment van dagvaarding afgerond neer op een bedrag van ongeveer € 25,-.

[255] Onder meer: Equifax Data Breach Class Action Settlement, *re Equifax Inc. Customer Data Security Breach Litigation*, Case No. 1:17-md-2800-TWT (N.D. Ga.); Plaintiffs' Unopposed motion for preliminary approval of class action settlement, *re Morgan Stanley Data Security Litigation*, Civil Action No. 1:20-cv-05914-AT.

512. In totaal komt dat uit op een bedrag van € 50,- aan materiële schade per Gedupeerde.

5.5 Bewijsaanbod schade

513. Gelet op de norm van artikel 82 AVG, het ruime schadebegrip, de verplichting tot AVG-conform interpreteren en op basis van de rechtspraak zoals hierboven behandeld, meent Stichting ICAM dat zij geen (verder) nadeel hoeft te concretiseren. Indien en zover uw rechtbank anders mocht oordelen, biedt Stichting ICAM hierbij aan (nader) bewijs te leveren van het bestaan en de omvang het geleden nadeel, zonder daarmee overigens enige bewijslast op zich te willen nemen die niet wettelijk op haar rust. Zij kan dat doen door representatief onderzoek onder de Gedupeerden te laten doen en deskundigenverklaringen te overleggen over het verlies van controle over persoonsgegevens, de psychologische gevolgen van het GGD-datalek, de tijd die wordt besteed aan het nemen van mitigerende maatregelen en een redelijke urenvergoeding.

6 AANSPRAKELIJKHEID

514. De aansprakelijkheid van de Staat c.s. vloeit zowel rechtstreeks voort uit de AVG (paragraaf 6.1) als (nevengeschikt) uit onrechtmatige daad (paragraaf 6.2) en uit hun aansprakelijkheid voor ondergeschikten op grond van artikel 6:170 BW (paragraaf 6.3). Onder iedere aansprakelijkheidsgrond bestaat een schadevergoedingsplicht ten aanzien van zowel materiële als immateriële schade. Stichting ICAM vordert primair de Staat zelfstandig en subsidiair de Staat c.s. hoofdelijk (paragraaf 6.4) te veroordelen om alle schade te vergoeden die de Gedupeerden hebben geleden ten gevolge van het GGD-datalek.

6.1 Aansprakelijkheid op grond van de AVG

6.1.1 Schendingen

515. Uit het geschetste in hoofdstuk 4 blijkt dat de Staat c.s. meerdere zwaarwegende verplichtingen uit de AVG hebben geschonden:

a) De beveiligingsplicht uit artikel 5(1)(f) AVG en artikel 32 AVG;

b) Het beginsel van dataminimalisatie uit artikel 5(1)(c) AVG;

c) De verantwoordingsplicht uit artikel 5 lid 2 AVG en artikel 24 AVG;

d) Beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen uit artikel 25 AVG;

e) De meldingsplicht van artikel 34 AVG.

6.1.2 Toerekenbaarheid, relativiteit en causaliteit

516. De Staat c.s. zijn op grond van de AVG aansprakelijk voor de schade die voortvloeit uit de schending van bovengenoemde verplichtingen. Het volgende is daarvoor redengevend.

517. Ten eerste dienen de inbreuken en de daardoor veroorzaakte schade aan de Staat althans de Staat c.s. te worden toegerekend. Uit artikel 82 lid 1 en 2 AVG volgt dat de verwerkingsverantwoordelijke aansprakelijk is voor schade die voortvloeit uit inbreuken op de AVG. Het gaat daarbij om een risicoaansprakelijkheid; niet relevant is of de verwerkingsverantwoordelijke een verwijt is te maken van de inbreuk. In deze zaak kwalificeert de Staat als verwerkingsverantwoordelijke, althans kwalificeren de Staat c.s. als gezamenlijk verwerkingsverantwoordelijken (paragraaf 4.2.1.2 en 4.2.1.3).

518. Ten tweede is voldaan aan het relativiteitsvereiste zoals besloten ligt in lid 2 van artikel 82 AVG. De artikelen 5, 24, 25, 32 en 34 AVG strekken immers specifiek tot bescherming tegen schade zoals die zich bij het GGD-datalek heeft voorgedaan (zie verder paragraaf 6.2.4)

519. Ten derde is het causaal verband tussen de overtredingen door de Staat c.s. en de schade van de Gedupeerden gegeven. Artikel 82 AVG voorziet immers in een risicoaansprakelijkheid: de verwerkingsverantwoordelijke is aansprakelijk indien een onrechtmatige verwerking van persoonsgegevens plaatsvindt, ongeacht of de verantwoordelijke verwijtbaar heeft gehandeld.[256] Dat betekent dat Stichting ICAM geen causaal verband hoeft aan te tonen. In dit geval hebben de Staat c.s. overigens wel degelijk verwijtbaar gehandeld.

520. Voor zover de rechtbank van oordeel is dat Stichting ICAM (ook) voor aansprakelijkheid onder de AVG (nader) zou moeten onderbouwen dat is voldaan aan de vereisten van toerekenbaarheid, relativiteit en causaliteit, verzoekt Stichting ICAM om hetgeen zij onder paragrafen 6.2.3, 6.2.4 en 6.2.5 aanvoert, hier als herhaald en ingelast te beschouwen.

[256] Rechtbank Noord-Nederland 12 januari 2021, ECLI:NL:RBNNE:2021:106 (*X/Oldambt*), r.o. 4.15. Zie ook: F.C. van der Jagt-Vink, 'Schadevergoeding onder de Algemene Verordening Gegevensbescherming', *MvV* 2019/7.9, p. 290.

6.2 Aansprakelijkheid op grond van onrechtmatige daad

521. De AVG laat eventuele eisen tot schadeloosstelling wegens inbreuken op andere regels in het Unierecht of het nationale recht van lidstaten onverlet.[257] Dat maakt dat Stichting ICAM haar vorderingen eveneens kan baseren op een onrechtmatige daad (artikel 6:162 BW).[258]

522. Ook wanneer de overheid een onrechtmatige daad pleegt, zoals in deze zaak, vindt toetsing plaats aan de hand van artikel 6:162 BW.[259] Dat artikel stelt verschillende vereisten voor het aannemen van aansprakelijkheid, waarbij Stichting ICAM opmerkt dat deze vereisten AVG-conform dienen te worden uitgelegd (paragraaf 6.2.1):

a) Er moet sprake zijn van een onrechtmatige daad (paragraaf 6.2.2);

b) De onrechtmatige daad moet aan de dader toegerekend kunnen worden (paragraaf 6.2.3);

c) De geschonden norm moet strekken ter bescherming tegen de veroorzaakte schade (relativiteit, paragraaf 6.2.4);

d) Er moet sprake zijn van een causaal verband tussen de onrechtmatige daad en de schade (paragraaf 6.2.5); en

e) Er moet sprake zijn van schade (hoofdstuk 5).

6.2.1 Artikel 6:162 BW dient AVG-conform te worden uitgelegd

523. Artikel 6:162 BW dient in deze zaak, voor zover nodig, te worden uitgelegd conform de AVG, op een wijze die ten volle recht doet aan de doelstellingen van de AVG. Het HvJEU heeft bepaald dat de nationale rechter gehouden is het van toepassing zijnde nationale recht zoveel mogelijk op een manier te interpreteren dat de effectieve werking van het Unierecht wordt verzekerd. Nationale normen dienen zoveel mogelijk te worden uitgelegd in het licht van de bewoordingen en het doel van het Unierecht.[260] Nu in deze zaak schendingen van het Unierecht centraal staan, ligt EU-conforme interpretatie van de onrechtmatige daad voor de hand. Dat betekent dat de beginselen en uitgangspunten van de AVG ten volle dienen te worden meegewogen bij de

[257] Overweging 146 bij de AVG.
[258] Groene Serie Onrechtmatige daad, par. 12.4.7.3 Verhouding van art. 82 van Verordening 2016/679 tot de onrechtmatige daad. Dit wordt ook bevestigd door de Afdeling in onder meer ABRvS 1 april 2020, ECLI:NL:RVS:2020:900, r.o. 25 op basis van de implementatietabel bij artikel 82 AVG in *Kamerstukken II* 2017/18, 34851 nr. 3.
[259] S.D. Lindenbergh, 'Commentaar op art. 6:162 BW', in: H.B. Krans, C.J.J.M. Stolker en W.L. Valk (red.), *Tekst & Commentaar Burgerlijke Wetboek,* Deventer: Wolters Kluwer.
[260] HvJEU 10 april 1984, ECLI:EU:C:1984:153 (*Von Colson en Kamann*), r.o. 26; HvJEU 20 september 2001, ECLI:EU:C:2001:465 (*Courage*), r.o 25; HvJEU 13 juli 2006, ECLI:EU:C:2006:461 (*Manfredi*), r.o. 87. Deze verplichting geldt ook voor Europese verordeningen: HvJEU 7 januari 2004, C-60/02 (*Rolex*), r.o. 59.

beoordeling van de vorderingen van Stichting ICAM c.s. op grond van onrechtmatige daad, zowel ten aanzien van de schendingen en de vereisten van toerekenbaarheid, relativiteit en causaal verband als ten aanzien van het vaststellen van het bestaan en de omvang van de schade.

6.2.2 Onrechtmatige daad

524. Ten eerste leveren de schendingen van de AVG door de Staat c.s. strijd op met een wettelijke plicht in de zin van artikel 6:162 BW lid 2 BW. Bij het handelen of nalaten in strijd met een wettelijk gebod of verbod moet niet alleen gedacht worden aan een wet in formele zin, maar aan elk algemeen bindend rechtsvoorschrift dat door het bevoegde gezag is uitgevaardigd. Ook Unieverordeningen zijn als zodanig te kwalificeren.[261] Verordeningen zoals de AVG zijn op grond van artikel 288 VWEU immers verbindend in al hun onderdelen en rechtstreeks toepasselijk in de lidstaten van de EU. Dat maakt dat de verplichtingen die voortvloeien uit de bepalingen in de AVG ook wettelijke plichten zijn binnen de rechtsstelsels van de afzonderlijke lidstaten.

525. Ten tweede leveren de schendingen van de AVG door de Staat c.s. strijd op met de maatschappelijke zorgvuldigheid in de zin van artikel 6:162 lid 2 BW. Maatschappelijke zorgvuldigheidsnormen zijn contextgebonden en flexibel van karakter. Deze normen moeten dan ook op basis van de concrete omstandigheden van het geval worden vastgesteld. Bij de toepassing van maatschappelijke zorgvuldigheidsnormen moeten een belangenafweging worden gemaakt tussen enerzijds het belang van de dader om het eigen belang na te streven en anderzijds het belang van het slachtoffer om niet de dupe te worden van schade die onrechtmatig is toegebracht.[262] Bij deze belangenafweging spelen de gerechtvaardigde verwachtingen van rechtszoekenden een doorslaggevende rol, bepalend is wat personen onderling in redelijkheid van elkaar kunnen verwachten.[263]

526. In de onderhavige zaak gaat het om een grootschalige verwerking van zeer gevoelige en bijzondere persoonsgegevens van burgers door de overheid. Burgers moeten erop kunnen vertrouwen dat de overheid zorgvuldig met hun persoonsgegevens omgaat, nu zij daaraan in feite overgeleverd zijn. Burgers mogen dan ook verwachten dat de systemen waarin hun persoonsgegevens opgeslagen worden, zoals in dit geval de GGD-systemen, adequaat beveiligd zijn. Op de overheid rust een zorgvuldigheidsverplichting om die adequate beveiliging te bewerkstelligen. Het nalaten om passende maatregelen te treffen om de persoonsgegevens van de 6,5 miljoen Gedupeerden te beveiligen, is in strijd met die zorgvuldigheidsnorm.

---

[261] C.H. Sieburgh, '44 1. Strijd met een wettelijke plicht.' in: *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel IV. De verbintenis uit de wet*., Deventer: Wolters Kluwer 2019; K.J.O. Jansen, '5.2.3 Verdragsbepalingen en Unierecht als wettelijke plichten', in: C.J.J.M. Stolker (red.), *Groene Serie Onrechtmatige daad*, Deventer: Wolters Kluwer.

[262] K.J.O. Jansen, 'Artikel 6:162 BW', in: C.J.J.M. Stolker (red.), *Groene Serie Onrechtmatige Daad,* Deventer: Wolters Kluwer.

[263] K.J.O. Jansen, 'Artikel 6:162 BW', in: C.J.J.M. Stolker (red.), *Groene Serie Onrechtmatige Daad,* Deventer: Wolters Kluwer.

6.2.3 Toerekenbaarheid

527. Het onrechtmatig handelen is toe te rekenen aan de Staat c.s. Artikel 6:162 lid 3 BW bepaalt dat een onrechtmatige daad aan de dader kan worden toegerekend indien zij te wijten is aan zijn schuld of aan een oorzaak welke krachtens de wet of de in het verkeer geldende opvattingen voor zijn rekening komt.

528. Ten eerste zijn het GGD-datalek en de AVG-schendingen die daaraan ten grondslag liggen te wijten aan de schuld van de Staat c.s. en deze dienen dan ook op die grond aan hen te worden toegerekend. De Staat c.s. hebben immers gedurende een lange periode nagelaten de persoonsgegevens in de GGD-systemen adequaat te beveiligen, zelfs nadat zij meerdere malen gewezen waren op tekortkomingen in de beveiliging (paragraaf 3.1.3).

529. Ten tweede moet het onrechtmatig handelen van de Staat c.s. op grond van de wet aan hen worden toegerekend, namelijk op grond van artikel 82 AVG. Artikel 6:162 BW dient in deze zaak AVG-conform te worden uitgelegd (paragraaf 6.2.1) en de AVG voorziet in een risicoaansprakelijkheid: de verwerkingsverantwoordelijke is aansprakelijk voor de schade ten gevolge van een AVG-inbreuk, ongeacht of hem daarvan een verwijt is te maken (paragraaf 6.1.2). In deze zaak kwalificeert de Staat als verwerkingsverantwoordelijke (paragraaf 4.2.1.1), althans kwalificeren de Staat c.s. in verschillende samenstellingen als gezamenlijk verwerkingsverantwoordelijken (paragraaf 4.2.1.2 en 4.2.1.3).

6.2.4 Relativiteit

530. Er is in deze zaak voldaan aan het relativiteitsvereiste. Artikel 6:163 BW bepaalt dat geen verplichting tot schadevergoeding bestaat als de geschonden norm niet strekt tot bescherming tegen schade zoals de benadeelde die heeft geleden.

531. De normen in de AVG strekken evident tot bescherming tegen de immateriële en materiële schade zoals de Gedupeerden deze hebben geleden.

532. In overwegingen 75 en 83 bij de AVG verwijst de Uniewetgever specifiek naar verschillende risico's waartegen verwerkingsverantwoordelijken passende maatregelen moeten nemen. Door niet te voldoen aan de belangrijke beveiligingsnormen die voortvloeien uit de AVG, hebben de Staat c.s. bovengenoemde risico's niet, althans onvoldoende, beperkt, waardoor een datalek heeft plaatsgevonden (een "inbreuk in verband met persoonsgegevens", paragraaf 4.2.3). Dat een datalek kan leiden tot schade zoals in onderhavig geval geleden door de Gedupeerden, blijkt uit overweging 85 bij de AVG:

> "Een inbreuk in verband met persoonsgegevens kan, wanneer dit probleem niet tijdig en op passende wijze wordt aangepakt, 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."

6.2.5 Causaliteit

533. Er is in de onderhavige zaak voldaan aan het vereiste causaal verband tussen het onrechtmatig handelen van de Staat c.s. en de schade die de Gedupeerden hebben geleden.

6.2.5.1 Ter inleiding: de problematiek van causaal verband bij schendingen van de AVG, in het bijzonder schendingen van de beveiligingsplicht

534. Vermogensschade als gevolg van een onrechtmatige daad komt voor vergoeding in aanmerking als de betrokkene "concrete schade" heeft geleden.[264] Het is doorgaans echter lastig vast te stellen of inadequate beveiliging van persoonsgegevens tot concrete schade voor Betrokkenen heeft geleid. Het is immers mogelijk dat schade pas na geruime tijd ontstaat doordat een crimineel bijvoorbeeld pas op een later moment misbruik maakt van de gelekte gegevens of deze gegevens pas op een later moment combineert met gegevens uit andere datalekken.[265]

535. Zelfs als wel concrete schade is geleden, is het volgende probleem dat het causaal verband tussen een schending van de AVG en de schade zich moeilijk laat aantonen, in het bijzonder waar het gaat om schendingen van de beveiligingsplicht. Zo kan het zijn dat persoonsgegevens door verschillende verwerkingsverantwoordelijken zijn gelekt, waardoor niet duidelijk is of de schade is ontstaan door het doen of nalaten van één bepaalde verwerkingsverantwoordelijke.[266] De Betrokkene verkeert ten aanzien van het aantonen van het causaal verband dan ook vaak in bewijsnood.

536. Er zijn verschillende mogelijkheden om een oplossing te bieden voor deze bewijsnood. Zo hebben verwerkingsverantwoordelijken onder de AVG een risicoaansprakelijkheid, waar in het licht van de AVG-conforme interpretatie van artikel 6:162 BW aansluiting bij gezocht zou moeten worden. Daarnaast dient het *condicio-sine-qua-non*-verband tussen de onrechtmatige daad en de schade in bepaalde gevallen te worden verondersteld. De leerstukken van redelijke toerekening, alternatieve causaliteit en proportionele aansprakelijkheid vormen andere oplossingen voor de problematiek rondom het causaal verband.

---

264 HR 18 januari 2002, ECLI:NL:HR:2002:AD4915 (*Interplant/Oldenburger*), r.o. 3.3.

265 T.F. Walree, *Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens*, (O&R nr. 126), diss. Nijmegen, Deventer: Wolters Kluwer 2021, p. 16-17.

266 T.F. Walree, *Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens*, (O&R nr. 126), diss. Nijmegen, Deventer: Wolters Kluwer 2021, p. 17-18.

6.2.5.2 Causaal verband hoeft niet aangetoond te worden

537. Stichting ICAM stelt zich primair op het standpunt dat zowel ten aanzien van de immateriële als de materiële schade zoals geleden door de Gedupeerden geen causaal verband aangetoond hoeft te worden. Het volgende is daarvoor redengevend.

538. Het aantonen van een causaal verband is ten aanzien van de beoordeling van immateriële schade overbodig, nu bij die beoordeling reeds naar de aard en de ernst van de schending en de gevolgen daarvan wordt gekeken (paragraaf 5.2.2). Het causaal verband maakt daarmee inherent onderdeel uit van de beoordeling van een vordering tot immateriële schadevergoeding. Een dergelijk causaal verband hoeft dan ook niet nogmaals separaat te worden vastgesteld.[267]

539. Bovendien is op grond van een AVG-conforme interpretatie van artikel 6:162 BW sprake van risicoaansprakelijkheid (paragraaf 6.1.2). Deze risicoaansprakelijkheid houdt in dat de Staat c.s. als verwerkingsverantwoordelijke aansprakelijk zijn voor de door de Gedupeerden geleden materiële en immateriële schade, zelfs als de schade is ontstaan door toedoen van een verwerker.

540. Verder dient het vereiste *condicio-sine-qua-non*-verband in beginsel te worden aangenomen indien een norm is geschonden die strekt tot bescherming tegen een specifiek gevaar, en juist dat gevaar zich heeft verwezenlijkt (de omkeringsregel).[268] De normen uit de AVG en in het bijzonder de beveiligingsnormen die voortvloeien uit de artikelen 5 en 32 AVG, strekken er specifiek toe Betrokkenen te beschermen tegen de gevolgen van datalekken en misbruik van persoonsgegevens (paragraaf 6.2.4). De Staat c.s. hebben nagelaten adequate maatregelen te nemen tegen deze gevaren, waardoor het risico op een datalek in de GGD-systemen zich daadwerkelijk heeft verwezenlijkt. Het *condicio-sine-qua-non*-verband tussen het onrechtmatig handelen door de Staat c.s. en de schade van de Gedupeerden is daarmee gegeven, behoudens tegenbewijs door de Staat c.s.

6.2.5.3 Causaal verband tussen onrechtmatig handelen door de Staat c.s. en schade aanwezig

541. Indien de rechtbank zou oordelen dat geen risicoaansprakelijkheid geldt en de omkeringsregel niet van toepassing zou zijn, stelt Stichting ICAM zich subsidiair op het standpunt dat er een causaal verband bestaat tussen het onrechtmatig handelen van de Staat c.s. en de schade zoals geleden door de Gedupeerden.

542. Het handelen, waaronder in het bijzonder het nalaten, van de Staat c.s. heeft tot gevolg gehad dat de persoonsgegevens van de Gedupeerden gecompromitteerd en buiten hun controle zijn

[267] T.F. Walree, *Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens*, (O&R nr. 126), diss. Nijmegen, Deventer: Wolters Kluwer 2021, p. 156.
[268] HR 29 november 2002, ECLI:NL:HR:2002:AE7345 (*TFS/NS*).

geraakt en deels daadwerkelijk zijn gestolen. Er is aldus sprake van een *condicio-sine-qua-non*-verband tussen het onrechtmatig handelen door de Staat c.s. en de schade zoals geleden door de Gedupeerden. Voor het aannemen van een *condicio-sine-qua-non*-verband is niet vereist dat absolute zekerheid bestaat over de vraag of de normschending de oorzaak is van de schade van de Gedupeerden. Een "redelijke mate van waarschijnlijkheid" is daartoe voldoende.[269]

543. Indien het handelen van de Staat c.s. wordt weggedacht, en er een hypothetische gevalsvergelijking wordt gemaakt met de situatie waarin het handelen van de Staat c.s. wel zou voldoen aan de (beveiligings)vereisten die voortvloeien uit de AVG, dan zouden de Gedupeerden geen schade hebben geleden.

544. Ten eerste is met een redelijke mate van waarschijnlijkheid vast te stellen dat de immateriële schade zoals Gedupeerden die hebben geleden is veroorzaakt door het onrechtmatig handelen van de Staat c.s. Gedupeerden hebben deze immateriële schade immers geleden doordat zij door de AVG-schendingen door de Staat c.s. de controle zijn verloren over hun (bijzondere) persoonsgegevens en gevoelens van stress, onrust en onbehagen ervaren (paragraaf 5.3). De immateriële schade is het directe gevolg van het datalek en de onzekerheid over wat er met de gegevens is gebeurd of nog zal gebeuren.

545. Ten tweede bestaat ook ten aanzien van de materiële schade zoals geleden door Gedupeerden een redelijke mate van waarschijnlijkheid dat het onrechtmatig handelen van de Staat c.s. daarvan de oorzaak is. Zo geven Gedupeerden aan sinds het datalek onder meer hun bankafschriften regelmatig te controleren en wachtwoorden te moeten vervangen (paragraaf 5.4). Naast het feit dat daarmee een tijdsinvestering gemoeid gaat, lenen de gegevens zoals buitgemaakt uit de GGD-systemen zich bij uitstek voor (identiteits)fraude, oplichting en andere criminele activiteiten (paragraaf 5.3.1.1). Er bestaat dan ook een redelijke mate van waarschijnlijkheid dat dergelijke schade die zich bij de Gedupeerden voordoet na het datalek uit de GGD-systemen, veroorzaakt is door het onrechtmatig handelen van de Staat c.s.

546. Ten derde kan de schade zoals geleden door de Gedupeerden aan de Staat c.s. worden toegerekend als een gevolg van het onrechtmatig handelen, zoals vereist door artikel 6:98 BW. Ook gelet daarop bestaat een causaal verband tussen het onrechtmatig handelen door de Staat c.s. en de schade zoals geleden door de Gedupeerden. Bij de beoordeling of de schade in zodanig verband staat met het onrechtmatig handelen door de Staat c.s. dienen alle omstandigheden van het geval te worden betrokken. Zo bepaalt het doel waarmee de beschermingsnorm in het leven geroepen is, de beschermingsomvang van de norm en daarmee ook of toerekening van de schade die in een concreet geval geleden is, gerechtvaardigd is. Naarmate bovendien de schuld aan het

[269] Zie onder meer: Conclusie A-G T. Hartlief 5 juli 2019, ECLI:NL:PHR:2019:826, bij HR 10 januari 2020, ECLI:NL:HR:2020:28, *NJB* 2020/187.

schadeveroorzakende feit groter is, is ruimere toekenning gerechtvaardigd.[270] Ook de voorzienbaarheid van de schade is een factor bij de redelijke toerekening.[271]

547. Vaststaat dat de Staat c.s. schuld hebben aan de schadeveroorzakende gebeurtenis. Zij hebben immers nagelaten adequate (beveiligings)maatregelen te treffen om de persoonsgegevens van de Gedupeerden te beschermen. Bovendien is de beveiligingsplicht uit de AVG mede in het leven geroepen om datalekken te voorkomen. De immateriële en materiële schade zoals geleden door de Gedupeerden is daarbij voorzienbaar, nu als algemeen bekend kan worden verondersteld dat gedupeerden van een datalek slachtoffer kunnen worden van criminele praktijken en dat een dergelijk lek bovendien zorgt voor verlies van controle over persoonsgegevens en gevoelens van stress, onrust en onbehagen oproept. Dat maakt dan ook dat de schade zoals geleden door de Gedupeerden in redelijkheid kan worden toegerekend aan de Staat c.s. als een gevolg van hun onrechtmatig handelen.

6.2.5.4 Alternatieve causaliteit

548. Voor zover de Staat c.s. zich erop zouden beroepen dat de immateriële en materiële schade zoals geleden door de Gedupeerden evengoed veroorzaakt zou kunnen zijn door andere oorzaken dan het GGD-datalek, zoals andere datalekken of de media-aandacht die aan het GGD-datalek is gegeven (zie paragraaf 3.1), doet Stichting ICAM een beroep op het leerstuk van alternatieve causaliteit. Artikel 6:99 BW bevat een omkering van de bewijslast voor gevallen waarin schade het gevolg kan zijn van verschillende gebeurtenissen waarvoor verschillende personen aansprakelijk zijn, maar in ieder geval door één van die gebeurtenissen daadwerkelijk is veroorzaakt. Ieder van de personen die aansprakelijk is voor de desbetreffende gebeurtenis is in dat geval verplicht tot vergoeding van de gehele schade, tenzij hij bewijst dat de schade niet door hem is veroorzaakt.[272]

549. In onderhavig geval leidt toepassing van het leerstuk van alternatieve causaliteit tot de conclusie dat de Staat c.s. aansprakelijk zijn voor de gehele immateriële en materiële schade zoals geleden door de Gedupeerden, zelfs als deze schade veroorzaakt zou zijn door een andere oorzaak dan het GGD-datalek. Dat is slechts anders als de Staat c.s. kunnen bewijzen dat de schade die Gedupeerden hebben geleden niet door hen veroorzaakt is.

---

[270] A.S. Hartkamp & C.H. Sieburgh, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands burgerlijk recht. 6. Verbintenissenrecht. Deel II. De verbintenis in het algemeen, tweede gedeelte*, Deventer: Wolters Kluwer 2021, paragraaf 63.

[271] A.S. Hartkamp & C.H. Sieburgh, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands burgerlijk recht. 6. Verbintenissenrecht. Deel II. De verbintenis in het algemeen, tweede gedeelte*, Deventer: Wolters Kluwer 2021, paragraaf 69.

[272] R.J.B. Boonekamp, 'Commentaar op art. 6:99 BW', in: A.T. Bolt (red.), *Groene Serie Schadevergoeding*, Deventer: Wolters Kluwer.

6.2.5.5 Proportionele aansprakelijkheid

550. Voor zover de Staat c.s. zich erop zouden beroepen dat de schade van de Gedupeerden ook veroorzaakt kan zijn door een oorzaak die in de risicosfeer van de Gedupeerde ligt, doet Stichting ICAM een beroep op het leerstuk van proportionele aansprakelijkheid. Op grond van de proportionele aansprakelijkheid kan aansprakelijkheid worden vastgesteld naar rato van waarschijnlijkheid dat de schade is ontstaan door het handelen of nalaten van de verwerkingsverantwoordelijke. In gevallen dat onzekerheid bestaat over het causaal verband en de kans niet zeer klein of zeer groot is dat de schade is veroorzaakt door het datalek, is het redelijk om deze onzekerheid te verdelen over de Betrokkene en de verwerkingsverantwoordelijke.[273]

551. Mocht aangenomen worden dat de door het GGD-datalek geleden schade gedeeltelijk in de risicosfeer van de Gedupeerden ligt, dan moet de onzekerheid over het causale verband aldus in redelijkheid verdeeld worden over de Gedupeerden en de Staat c.s. Voor het geval de rechtbank zou oordelen dat van een dergelijke situatie sprake is, biedt Stichting ICAM hierbij aan bewijs te leveren van een redelijke verdeling, zonder daarmee overigens enige bewijslast op zich te willen nemen die niet wettelijk op haar rust.

6.2.6 Schade

552. Zoals uiteengezet in hoofdstuk 5 hebben Gedupeerden schade geleden door het onrechtmatig handelen van de Staat c.s.

6.3 Risicoaansprakelijkheid voor ondergeschikten

553. De Staat c.s. zijn voorts aansprakelijk op grond van artikel 6:170 BW. Artikel 6:170 BW bepaalt dat een werkgever risicoaansprakelijk is voor de schade die aan een derde is toegebracht door een fout van zijn werknemers wanneer de kans op de fout door de opdracht tot het verrichten van de taak is vergroot en de werkgever zeggenschap had over de gedraging waarin de fout was gelegen. De in de wet bedoelde fout moet worden uitgelegd als een onrechtmatige gedraging als bedoeld in artikel 6:162 BW.

554. Om deze aansprakelijkheid aan te kunnen nemen is nodig dat de werknemer(s) van de GGD'en zelfstandig een onrechtmatige daad op grond van artikel 6:162 BW hebben begaan. Voorts vereist artikel 6:170 BW dat er een functioneel verband is tussen de werkzaamheden en de fout en moet de werkgever zeggenschap hebben gehad. Stichting ICAM houdt de Staat c.s. dan ook risicoaansprakelijk voor het lekken van de persoonsgegevens als degenen onder wiens

[273] T.F. Walree, *Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens*, (O&R nr. 126), diss. Nijmegen, Deventer: Wolters Kluwer 2021, p. 19.

zeggenschap de medewerkers van de GGD'en hun taak hebben vervuld. Hiertoe voert Stichting ICAM het volgende aan.

555. In onderhavige zaak hebben medewerkers van de GGD'en ongeoorloofd inzage genomen in de persoonsgegevens van Gedupeerden en een onbekend aantal van hen heeft gegevens daadwerkelijk ontvreemd, te koop aangeboden en/of verkocht. Dit is evident te kwalificeren als een onrechtmatige gedraging, gelegen in een strijd met een wettelijke plicht en met een maatschappelijke zorgvuldigheidsnorm. Door deze onrechtmatige gedraging is een ernstige inbreuk gemaakt op de persoonlijke levenssfeer van de Gedupeerden.[274] Deze gedraging is bovendien toerekenbaar aan de medewerkers. De medewerkers wisten of behoorden te weten dat wat zij deden niet alleen onrechtmatig was, maar ook een groot risico op een datalek met zich meebracht. Voor zover de Staat c.s. zich op het standpunt stellen dat de medewerkers hiermee hebben gehandeld in strijd met de instructies van de werkgever, waardoor de aansprakelijkheid zou ontvallen, merkt Stichting ICAM op dat de aansprakelijkheid als bedoeld in artikel 6:170 BW een risicoaansprakelijkheid is zodat er geen gelegenheid bestaat tot disculpatie.[275]

556. Stichting ICAM is derhalve van mening dat de gedraging van de werknemers een toerekenbare onrechtmatige daad tot gevolg heeft, waarvoor de werkgever risicoaansprakelijk is.

557. Daarnaast is een functioneel verband vereist tussen de fout van de werknemer enerzijds en de taak die hem is opgedragen anderzijds. Dit verband moet op grond van de rechtspraak ruim worden opgevat.[276] De GGD-medewerkers hadden in het kader van hun werkzaamheden toegang tot de dossiers en hebben onder werktijd, binnen de werkomgeving en door gebruik te maken van de aan hen ter beschikking gestelde toegang/autorisatie, inzage gehad. De Staat c.s. hadden daarbij zeggenschap over de gedraging(en) waarvan de fout deel uitmaakte, zij hadden immers grote invloed op de inrichting van het proces en de wijze waarop taken uitgevoerd moest worden.

558. Voor zover de Staat c.s. zich op het standpunt stellen dat zij niet aangemerkt kunnen worden als werkgever, merkt Stichting ICAM op dat het feit dat de Staat c.s. een deel van de medewerkers heeft ingehuurd via externe callcenters, onverlet laat dat de Staat c.s. kunnen worden gekwalificeerd als degenen onder wiens gezag de medewerkers hun taak vervulden. De rechtspraak gaat uit van een cumulatieve aansprakelijkheid tenzij uit de onderlinge rechtsverhouding iets anders blijkt.[277]

[274] Zie in dit verband ook: Rb. Zeeland West-Brabant, 21 september 2022, ECLI:NL:RBZWB:2022:5457, r.o. 4.4.
[275] Rb Rotterdam 11 oktober 2019, ECLI:NL:RBROT:2019:7863, r.o. 4.2.
[276] Rb. Zeeland West-Brabant, 21 september 2022, ECLI:NL:RBZWB:2022:5457, r.o. 4.9.
[277] Zie: HR 15 juni 1990, *NJ* 1990/716 (Stormer/Vedox)

6.4 Hoofdelijke aansprakelijkheid

559. Artikel 82 lid 4 AVG bepaalt dat wanneer meer dan één verwerkingsverantwoordelijke bij dezelfde inbreukmakende verwerking betrokken is, zij gezamenlijk en hoofdelijk aansprakelijk zijn. Op grond van lid 5 kunnen zij regres op elkaar nemen. Voor zover de rechtbank zou oordelen dat de Staat niet zelfstandig als verwerkingsverantwoordelijke dient te worden aangemerkt is, maar de Staat c.s. gezamenlijk, geldt dus dat zij hoofdelijk aansprakelijk zijn.

560. Artikel 6:102 BW bepaalt dat wanneer op twee of meer personen een verplichting tot vergoeding van dezelfde schade rust, zij hoofdelijk zijn verbonden deze schade te vergoeden. Daarvoor is niet vereist dat de aansprakelijkheid van deze verschillende personen op dezelfde rechtsgrond berust. Artikel 6:102 BW is van toepassing op wettelijke verplichtingen tot schadevergoeding, waaronder op de verplichting tot schadevergoeding die voortvloeit uit onrechtmatige daad.[278] Ook de (U)AVG bevat een wettelijke verplichting tot schadevergoeding, waarop artikel 6:102 BW aldus van toepassing is.

561. Op grond van het bepaalde in artikel 6:7 lid 1 BW zijn de personen die hoofdelijk aansprakelijk zijn, ieder gehouden tot vergoeding van de gehele schade jegens de benadeelde. Betaling door de één, bevrijdt de ander. Degene die als eerste wordt aangesproken, kan niet het verweer voeren dat de benadeelde geen schade heeft omdat hij een verhaalbare vordering heeft op een andere aansprakelijke.[279]

562. De Staat c.s. zijn op grond van het bovenstaande dan ook hoofdelijk aansprakelijk om de gehele schade zoals geleden door de Gedupeerden te vergoeden.

7 VERWEREN EN WEERLEGGING

563. Stichting ICAM is niet bekend met andere verweren van de Gedaagden dan zoals besproken tijdens de mondelinge overleggen met GGD GHOR en de Staat op 6 april resp. 19 april 2022 en in de brieven van 13 en 25 resp. 24 mei 2022 (**producties H.2J, H.2K en H.1E**). Zij voeren in de kern de volgende verweren:

a) De ideële doelstelling van Stichting ICAM zou niet rijmen met de ingestelde vordering. Deze zou slechts een verdienmodel voor de procesfinancier faciliteren;

b) Het gekozen middel zou niet geschikt zijn voor het bereiken van de doelstelling;

[278] R.J.B. Boonekamp, 'art. 6:102 BW, aant. 1.3 Reikwijdte en toepassingsgebied', in: A.T. Bolt (red.), *Groene Serie Schadevergoeding* Deventer: Wolters Kluwer.
[279] R.J.B. Boonekamp, 'art. 6:102 BW, aant. 1.4 Hoofdelijkheid', in: A.T. Bolt (red.), *Groene Serie Schadevergoeding* Deventer: Wolters Kluwer.

c) De gevorderde schade dient door Stichting ICAM concreet onderbouwd te worden; en

d) Stichting ICAM zou geen causaal verband kunnen aantonen tussen het datalek en de schade.

7.1 Ideële doelstelling Stichting ICAM

564. GGD GHOR en de Staat trekken beide de ideële doelstelling van Stichting ICAM in twijfel en trachten deze zaak weg te zetten als een poging een verdienmodel te faciliteren voor de procesfinancier. Kort weergegeven is de reden hiertoe gelegen in het feit dat zij slecht zouden inzien hoe dit specifieke geval kan leiden tot het verbeteren van de informatiebeveiliging bij de overheid in algemene zin. Het instellen van de vorderingen zou ineffectief zijn, nu dat doel niet binnen de invloedssfeer van de Gedaagden zou liggen.

565. Stichting ICAM betreurt het dat GGD GHOR en het ministerie veel aandacht besteden aan het in twijfel trekking van de ideële doelstelling van Stichting ICAM. Zij wekken hiermee de indruk zich niet bewust te zijn van de enorme impact die het GGD-datalek op de Gedupeerden en de maatschappij als geheel heeft gehad. GGD GHOR en het ministerie waren reeds bekend met de problemen in de beveiliging. Doordat zij onvoldoende hebben gehandeld is een situatie gecreëerd waarin gegevens van zeker 1.250 mensen in het criminele circuit zijn beland en potentieel zelfs van miljoenen Gedupeerden. Dat GGD GHOR en het ministerie wat dat betreft de hand niet in eigen boezem steken, acht Stichting ICAM kwalijk.

566. Stichting ICAM heeft in haar brief van 4 mei 2022 duidelijk uiteengezet welk doel zij nastreeft met deze collectieve actie. Het doel is primair ideëel. Stichting ICAM streeft met de collectieve actie naar een bijdrage aan het volledig dichten van het datalek, zoveel mogelijk helderheid over wat er is gebeurd, het stimuleren van de overheid om in zijn algemeenheid zorgvuldiger om te gaan met persoonsgegevens en het bevorderen dat de overheid betere preventieve maatregelen treft voor de bescherming van persoonsgegevens. Dit zijn naar mening van Stichting ICAM nastrevenswaardige doelen die ook passen binnen de doelstellingen van de WAMCA, namelijk het in de gelegenheid stellen van burgers om civielrechtelijke handhavingsmaatregelen te treffen, waar maatregelen van de overheid zelf tekort schieten. Dat doel wordt ook onderschreven door de Europese wetgever.[280]

567. Voorts is het onjuist dat een specifiek geval of incident geen aanleiding kan zijn om de ideële doelstelling van Stichting ICAM te bereiken. Als blijkt dat de Staat c.s. aansprakelijk zijn voor de schade ten gevolge van het GGD-datalek, gaat een boodschap uit naar (overheids)instanties dat, indien zij hun zaken niet op orde hebben, hier daadwerkelijk gevolgen aan worden verbonden. Een specifiek geval als dit dient daarom een cruciale functie in het bewegen van

[280] Europese richtlijn Representatieve vorderingen ter bescherming van de collectieve belangen van consumenten, (EU) 2020/1828

overheidsinstanties om adequaat te handelen, ook in een crisissituatie. Het functioneert als katalysator voor verandering binnen de overheid in brede zin. Zij kan dan niet langer stilzitten en zal actief moeten gaan handelen. Daarbij dient te worden opgemerkt dat het beschermen van persoonsgegevens vanuit de overheid in brede zin van groot algemeen belang is. Het GGD-datalek betreft het grootste datalek in de Nederlandse geschiedenis, waarbij het gaat om (zeer) gevoelige gegevens en er sprake was van een ernstig verwijtbare overtreding. Van een specifiek geval, in het bijzonder het GGD- datalek, kan derhalve een belangrijke signaalfunctie uitgaan naar andere overheidsinstanties om de beveiliging van de systemen (ook) op orde te brengen.

568. Dat deze zaak wordt gefinancierd door een commerciële procesfinancier doet aan het voorgaande niet af. Zonder de hulp van een financier – die een aanzienlijk risico neemt – zouden zaken zoals deze waarschijnlijk nooit gevoerd worden. Daarvoor zijn de kosten simpelweg te hoog in vergelijking met de individuele financiële belangen. Dat de financier een vergoeding wil voor het risico dat hij neemt, is ook niet meer dan logisch. De Financier van deze zaak is daarbij in het geheel niet uit op woekerwinsten. Liesker Procesfinanciering heeft uit eigen initiatief voorgesteld om haar vergoeding te maximeren tot een bedrag ter hoogte van vijfmaal de door haar geïnvesteerde som, terwijl in collectieve acties met een aanzienlijke omvang een percentage van 20-25% van de opbrengst over het algemeen aanvaardbaar wordt geacht.

7.2 Gekozen middel

569. GGD GHOR stelt dat een massaclaim niet het juiste instrument zou zijn om het ideële doel van Stichting ICAM te bereiken. Stichting ICAM wenst immers het datalek te dichten en helderheid te verkrijgen over wat er is gebeurd. GGD GHOR is van mening dat een massaclaim hiertoe niet effectief zou zijn aangezien het datalek al de volledige aandacht heeft van de politie en de AP een onderzoek heeft ingesteld (**producties H.2J en H.2K**).

570. Privaatrechtelijke handhaving, door middel van het instellen van een schadevordering, is in het onderhavige geval echter van groot belang. Hoewel de AP een onderzoek heeft verricht, heeft zij ook al ten kennen gegeven niet handhavend op te zullen gaan treden. Ook uit eerdere incidenten is niet in passende mate gebleken dat de overheid dit probleem serieus neemt, voorgaande onderzoeken van de AP hebben niet geleid tot een overheidsbreed betere informatiebeveiliging. Een collectieve actie waaraan een financiële prikkel tot nakoming wordt verbonden lijkt daarmee het enige resterende middel om de overheid tot verandering te bewegen.

571. Ook wanneer de AP wél zou overgaan tot het opleggen van een (aanzienlijke) boete, biedt dit overigens geen genoegdoening voor de Gedupeerden. Stichting ICAM is er principieel van overtuigd dat ten gevolge van het datalek vergoedbare schade is geleden door iedereen van wie gegevens in de IT-systemen van de GGD'en waren of zijn opgenomen.

7.3 Concrete onderbouwing van de schade

572. Zowel GGD GHOR als het ministerie stellen dat Stichting ICAM de gevorderde schade concreet dient te onderbouwen. Dit is onjuist. Een persoonsaantasting in de zin van artikel 6:106 lid 1 aanhef en onder b BW vereist geen concrete onderbouwing van de schade 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 (paragraaf 5.2.2).

7.4 Causaal verband

573. Tijdens het mondelinge overleg tussen (de advocaten van) Stichting ICAM en (de advocaten van) de Staat op 19 april 2022, heeft de Staat ten slotte het verweer aangevoerd dat geen causaal verband kan worden aangetoond tussen het GGD-datalek en door de Gedupeerden geleden materiële of immateriële schade. Zo die schade al zou bestaan, zou die immers evengoed veroorzaakt kunnen zijn door een ander datalek of door het enkele feit dat mensen zelf persoonsgegevens hebben gedeeld via bijvoorbeeld sociale media, aldus de Staat. Het verweer snijdt geen hout, en de Staat lijkt zich daar in de brief van haar advocaat van 24 mei 2022 (**productie H.1E**) ook van bewust te zijn geworden. In de hierboven omschreven toets is causaal verband immers een gegeven: de nadelige gevolgen voor de benadeelde liggen zo voor de hand, dat een aantasting in de persoon kan worden aangenomen.

8 BEWIJSLAST EN BEWIJS

574. De bewijslast ten aanzien van de AVG-overtredingen in deze zaak ligt bij de Staat c.s. Op basis van artikel 5 lid 2 AVG hebben de Staat c.s. immers een verantwoordingsplicht die met zich meebrengt dat op hen de plicht rust om de naleving van de AVG aan te tonen (zie paragraaf 4.2.2). De verantwoordingsplicht vertaalt zich in deze procedure in een bewijslast voor de Staat c.s. dat zij de AVG niet heeft geschonden.

575. Ondanks deze bewijslastverdeling heeft Stichting ICAM in deze Dagvaarding uitgebreid uiteengezet hoe de Staat c.s. de AVG hebben geschonden. Dit leidt tot een verdere verhoging van de plicht van de Staat c.s. om hun eventueel verweer te onderbouwen met bewijs.

576. Stichting ICAM heeft in deze Dagvaarding voldaan aan haar stelplicht en de aanwezigheid van de door haar gestelde feiten voldoende aannemelijk gemaakt. Indien en voor zover de rechtbank toch van oordeel zou zijn dat Stichting ICAM niet geslaagd is het benodigde bewijs te leveren, biedt zij hierbij bewijs aan van al haar stellingen met alle middelen die rechtens tot haar beschikking staan, zonder dat zij daarmee overigens vrijwillig enige bewijslast op zich neemt die niet rechtens op haar rust. Stichting ICAM biedt onder andere bewijs aan door het horen van getuigen en het in het geding brengen van nadere stukken.

577. Met name biedt Stichting ICAM bewijs aan door middel van deskundigenverklaringen en getuigenverhoren, zoals ten aanzien van:

a) De gebrekkige beveiliging van de GGD-systemen;

b) De psychologische effecten van datalekken zoals het GGD-datalek en de daardoor veroorzaakte immateriële schade;

c) De omvang van de door de Gedupeerden geleden schade;

d) Het aanbieden en verhandelen van grote databestanden afkomstig uit de GGD-systemen door (cyber-)criminelen;

e) De omvang van de groep personen waarvan vaststaat dat gegevens ongeoorloofd zijn ingezien en/of ontvreemd, en/of de mate van (on)zekerheid of dat het geval is; en

f) Het bestaan en de omvang van de groep Deelnemers.

578. Ten aanzien van de onderwerpen sub a), d) en e) geldt dat de feiten die in dat kader eventueel bewezen moeten worden, voor een groot deel buiten het bereik en zicht liggen van Stichting ICAM en eventuele deskundigen. Zo heeft Stichting ICAM geen toegang tot de GGD-systemen en (vooralsnog) geen inzage in bijvoorbeeld logbestanden, het forensisch rapport van Fox-IT (paragraaf 3.4), de voortgangsrapportage naar aanleiding van het onderzoek van de AP naar de GGD-systemen (paragraaf 3.5) of de uitkomsten van het politieonderzoek (paragraaf 3.4). Ten aanzien van het verhandelen van grote bestanden in het criminele circuit waaronder op het darkweb, beschikken journalisten van RTL Nieuws over informatie.

579. Ten aanzien van deze onderwerpen, en indien en voor zover zou worden geoordeeld dat de bewijslast ter zake op Stichting ICAM rust, verzoekt zij de rechtbank dan ook aan dit bezwaar en haar alsdan bestaande bewijsnood tegemoet te komen, zoals door middel van het aannemen van een feitelijk vermoeden, het verdelen of omkeren van de bewijslast, door de Staat c.s. te onderwerpen aan een verzwaarde stel- of motiveringsplicht, door de omkeringsregel toe te passen ten aanzien van het causaal verband tussen onrechtmatig handelen en schade (voor zover dit beoordeeld zou moeten worden op basis van artikel 6:162 BW en artikel 6:162 BW niet AVG-conform zou moeten worden uitgelegd) of door middel van het bevelen van de Staat c.s. om alle van belang zijnde feiten volledig en naar waarheid aan te voeren, haar verweren toe te lichten of bepaalde, op de zaak betrekking hebbende bescheiden over te leggen, zulks op grond van artikel 21 en 22 Rv.[281]

[281] Zie bijvoorbeeld Hoge Raad 8 juli 2022, ECLI:NL:HR:2022:1058.

580. Voor zover de rechtbank dit verzoek niet honoreert, biedt Stichting ICAM aan bewijs te leveren door middel van getuigenverhoren. De volgende getuigen zouden kunnen verklaren over de onderwerpen sub a), d) en e):

a) [redacted]: de RTL-journalist die het GGD-datalek aan het licht bracht;

b) [redacted]: vanaf september 2020 adjunct-directeur GGD GHOR, naar eigen zeggen vanaf het begin betrokken geweest bij de afhandeling van het datalek;

c) [redacted]: vanaf augustus 2021 interim CIO (Chief Information Officer) bij GGD GHOR, vanuit die rol waarschijnlijk goed geïnformeerd over het datalek en de gevolgen daarvan;

d) [redacted]: DPG GGD Zuid-Holland Zuid en lid van het Dagelijks Bestuur van GGD GHOR, was aanwezig bij de overleggen met GGD GHOR, gelet daarop en vanuit zijn rol waarschijnlijk goed geïnformeerd over het datalek en de gevolgen daarvan;

e) [redacted]: DPG GGD Haaglanden Zuid, was aanwezig bij de overleggen met GGD GHOR, gelet daarop waarschijnlijk goed geïnformeerd over het datalek en de gevolgen daarvan;

f) [redacted]: DPG GGD Hollands Noorden, was aanwezig bij de overleggen met GGD GHOR, gelet daarop waarschijnlijk goed geïnformeerd over het datalek en de gevolgen daarvan

g) [redacted]: DPG GGD Amsterdam en lid van het DB van GGD GHOR, vanuit die rol waarschijnlijk goed geïnformeerd over het datalek en de gevolgen daarvan;

h) [redacted]: van januari 2017 tot en met mei 2022 CIO bij het ministerie van VWS, vanuit die rol waarschijnlijk goed geïnformeerd over het datalek en de gevolgen daarvan;

i) [redacted]: voormalig beleidsmedewerker ministerie van VWS. Een anonieme brievenschrijver schrijft: “Over de GGD-systemen sprak iedereen als ‘zo lek als een mandje’. De rechterhand van CIO [redacted], mevrouw [redacted], heeft in ieder geval één keer gezegd dat zij vond dat de ClO moest ingrijpen, maar hij wilde dat niet. Zij is kort daarna vertrokken. Volgens de geruchten met ruzie met [redacted]. Mevrouw [redacted] werkt er nog wel en die was er ook bij. Zij moet dit dus ook weten.”;

j) [redacted]: tussen januari 2020 en januari 2022 achtereenvolgend waarnemend plaatsvervangend CIO Directie Informatiebeleid/CIO en coördinerend/specialistisch adviseur informatiebeleid, zie het citaat uit de brief hierboven;

k) [redacted]: vanaf november 2019 Team Lead Forensics bij Fox-IT, vanuit die rol waarschijnlijk goed geïnformeerd over het datalek en de gevolgen daarvan.

581. Indien de rechtbank overweegt een bewijsopdracht te geven aan Stichting ICAM, dan verzoekt zij dit te combineren met een opdracht aan de Staat c.s. om aan Stichting ICAM alle noodzakelijke gegevens te verschaffen.

582. Stichting ICAM biedt voorts aan tegenbewijs te leveren, door alle middelen rechtens, waaronder getuigenbewijs, voor zover stellingen van de Staat c.s. (voorlopig) als juist worden aangenomen door de rechtbank.

9 ARTIKEL 3:305A EN DE WAMCA: ONTVANKELIJKHEID EN VEREISTEN

583. Het GGD-datalek vond plaats in de periode vanaf de inzet van de GGD-systemen in de coronapandemie en derhalve tussen februari 2020 en heden. Op grond van artikel III lid 2 WAMCA vindt de WAMCA toepassing op collectieve vorderingen die zijn ingesteld na 1 januari 2020 en die betrekking hebben op gebeurtenissen op of na 15 november 2016. De WAMCA is daarmee dus van toepassing op deze collectieve procedure.

584. Stichting ICAM voldoet aan alle vereisten van artikel 3:305a BW en is dus ontvankelijk om deze collectieve actie als belangenbehartiger van de Gedupeerden te voeren. Stichting ICAM stelt zich daarbij op het standpunt dat zij voor alle Gedupeerden van het GGD-datalek kan optreden en dat artikel 80 lid 2 AVG daaraan niet in de weg staat (paragraaf 9.2.2).

585. In het navolgende zal Stichting ICAM eerst toelichten dat zij voldoet aan de ontvankelijkheidseisen op grond van artikel 3:305a BW en aan de principes uit de Claimcode 2019 (paragraaf 9.1). Daarna zal zij uitleggen waarom artikel 80 AVG geen beletsel vormt voor deze collectieve actie (paragraaf 9.2). Vervolgens zal Stichting ICAM toelichten dat, zelfs als artikel 80 AVG wel een beletsel vormt, zij onder de WAMCA toch ontvankelijk is aangezien zij haar vorderingen ook baseert op een onrechtmatige daad (paragraaf 9.3). Tenslotte zal zij een toelichting geven op de vereisten van artikel 1018c Rv (paragraaf 9.4).

9.1 Stichting ICAM is ontvankelijk onder artikel 3:305a BW

586. Met de inwerkingtreding van de WAMCA zijn de ontvankelijkheidseisen van artikel 3:305a BW aangescherpt. Dat is met name gebeurd om oneigenlijk gebruik van de collectieve actie te voorkomen.[282] Om die reden dient de rechter terughoudend te toetsen aan de ontvankelijkheidseisen. Belangenorganisaties hebben immers de vrijheid om hun eigen organisatie in te richten. Het recht op toegang tot de rechter mag niet lichtvaardig worden

[282] *Kamerstukken II* 2017/18, 34 608, 9, p.1.

beperkt. Ontvankelijkheidsverweren, die er vaak vooral op zijn gericht om te ontkomen aan de hoofdzaak, dienen daarentegen kritisch benaderd te worden.

587. Artikel 3:305a lid 1 BW bepaalt dat een belangenorganisatie:

a) Een rechtsvordering kan instellen die strekt tot bescherming van gelijksoortige belangen van andere personen (paragraaf 9.1.1);

b) Voor zover zij deze belangen ingevolge haar statuten behartigt (paragraaf 9.1.2); en

c) Voor zover met de rechtsvordering de belangen van de personen ten behoeve van wie de vordering is ingesteld voldoende zijn gewaarborgd. Dit vereiste is verder uitgewerkt in artikel 3:305a lid 2 BW (paragraaf 9.1.3).

588. Artikel 3:305a lid 3 BW bevat een aantal aanvullende ontvankelijkheidseisen (paragraaf 9.1.4):

a) Bestuurders betrokken bij de oprichting van een belangenorganisatie en hun opvolgers, mogen geen rechtstreeks of middellijk winstoogmerk hebben dat via de belangenorganisatie wordt verwezenlijkt (paragraaf 9.1.4.1);

b) De collectieve vordering dient een voldoende nauwe band met de Nederlandse rechtssfeer te hebben (paragraaf 9.1.4.2); en

c) De belangenorganisatie dient in de gegeven omstandigheden voldoende te hebben getracht het gevorderde te bereiken door het voeren van overleg met de gedaagden (paragraaf 9.1.4.3).

9.1.1 Gelijksoortige belangen die zich voor bundeling lenen

589. Uit vaste rechtspraak van de Hoge Raad volgt dat het vereiste van gelijksoortigheid vervuld is wanneer de belangen ter bescherming waarvan de vordering strekt, zich lenen voor bundeling, zodat een efficiënte en effectieve rechtsbescherming ten behoeve van de belanghebbenden kan worden bevorderd. De vorderingen lenen zich voor bundeling als daarover in één procedure geoordeeld kan worden zonder naar de bijzondere omstandigheden van de individuele belanghebbenden te kijken.[283] De eis van voldoende gelijksoortigheid brengt volgens de Hoge Raad niet mee dat de posities, achtergronden en belangen van degenen voor wie de collectieve actie wordt ingesteld identiek of zelfs overwegend gelijk zijn. De Hoge Raad acht een zekere abstrahering van concrete individuele gevallen dan ook passend in een collectieve actie.[284]

[283] HR 26 februari 2010, ECLI:NL:HR:2010:BK5756 (*Stichting Baas in Eigen Huis/Plazacasa).*
[284] HR 27 november 2009, ECLI:NL:HR:2009:BH2162 (*WorldOnline*), r.o. 4.8 ; zie ook: D.L. Barbiers, 'Beoordeling van schadevergoedingsvorderingen door de rechter in collectieve actie', *NTBR* 2020, afl. 8.

590. De belangen van de Gedupeerden bij de vorderingen die Stichting ICAM in deze procedure instelt, zijn gelijksoortig en lenen zich bij uitstek voor bundeling.

591. De Gedupeerden zijn allemaal getroffen door dezelfde onrechtmatige handelingen van de Staat c.s., als gevolg waarvan zij dezelfde, forfaitair vast te stellen immateriële en materiële schade hebben geleden, zij het in twee categorieën. Het gaat in alle gevallen om schendingen van artikel 8 EVRM, artikel 7 en 8 Handvest en artikel 5, 24, 25, 32 en 34 AVG en onrechtmatig handelen op grond van artikel 6:162 BW, artikel 6:170 BW en specifieke zorgwetgeving, ten gevolge van dezelfde feitelijke handelingen. De door Stichting ICAM aangevoerde schendingen raken ieder der Gedupeerden in gelijke mate, althans ieder der Gedupeerden binnen ieder van de verschillende categorieën Gedupeerden (zie paragraaf 9.1.3.1).

592. Voor toewijzing van de vorderingen van Stichting ICAM is dan ook geen individuele beoordeling van de persoonlijke omstandigheden van de (subgroepen van) Gedupeerden nodig, maar enkel een algemene beoordeling van het handelen en de aansprakelijkheid van de Staat c.s. Dat geldt zowel voor de vordering tot een verklaring voor recht, de vordering tot schadevergoeding als de vorderingen die zien op herstel van de overtredingen.

593. De conclusie dat de belangen van de Gedupeerden in deze zaak voldoende gelijksoortig zijn, wordt ondersteund door een uitspraak van de rechtbank Amsterdam d.d. 30 juni 2021 in de (WCAM-) procedure tussen de Data Privacy Stichting en Facebook. De rechtbank oordeelde dat de gevorderde verklaringen voor recht een efficiënte rechtsbedeling bevorderen en dat de daarbij betrokken belangen zich lenen voor bundeling:

> “De vraag of de bij de vorderingen betrokken belangen zich voor bundeling lenen, hangt mede af van de aard van de ingestelde vorderingen. De vorderingen van de Stichting beperken zich tot verklaringen voor recht dat sprake is van onrechtmatig handelen, oneerlijke handelspraktijken en ongerechtvaardigde verrijking. Anders dan in enkele van de uitspraken waarnaar Facebook c.s. heeft verwezen, vordert de Stichting bijvoorbeeld geen verklaring voor recht die verband houdt met dwaling, bij de beoordeling waarvan eerder individuele omstandigheden van belang zijn.
> De vorderingen van de Stichting hebben betrekking op diverse voldoende nauw omschreven handelwijzen van Facebook c.s. Die vorderingen zijn er in de kern op gebaseerd dat Facebook c.s. de privacy van haar gebruikers (voor zover behorend tot de achterban) heeft geschonden doordat zij zonder de benodigde toestemming persoonsgegevens heeft verwerkt. Met de ingestelde vorderingen wenst de Stichting zodoende een oordeel over de vraag of persoonsgegevens van (bepaalde) gebruikers van de Facebook-dienst in overeenstemming met de regelgeving zijn verwerkt. Een dergelijk oordeel over de (on)rechtmatigheid van de handelwijze van Facebook c.s. ten aanzien van de verwerking van persoonsgegevens leent zich voor een collectieve actie.
> […]
> Anders dan Facebook c.s. heeft betoogd, bevordert bundeling van de belangen van de achterban van de Stichting ook een efficiënte en effectieve rechtsbescherming. De algemene vraag naar de onrechtmatigheid van de gestelde handelwijze en de aansprakelijkheid van Facebook c.s kan in deze collectieve procedure immers worden beantwoord. Daarmee is deze collectieve procedure efficiënter dan het op individuele basis voeren van procedures over de rechtmatigheid van de

> gegevensverwerking door Facebook c.s. Ook is duidelijk dat de individuele belanghebbenden voor wie de Stichting opkomt, onmiskenbaar baat hebben bij toewijzing van de door de Stichting gevorderde verklaringen voor recht. Aan het voorgaande doet niet af dat een individuele belanghebbende op basis van een eventuele toewijzing van de gevorderde verklaringen voor recht in deze collectieve actie niet zonder meer aanspraak kan maken op schadevergoeding en dat daarvoor mogelijk een (individuele) vervolgprocedure nodig is."[285]

594. Er bestaan tussen de (verschillende groepen) Gedupeerden wel feitelijke verschillen, gelegen in de volgende omstandigheden:

a) Bij welke GGD de Gedupeerde een afspraak heeft gemaakt voor testen of vaccineren en/of in welke GGD-regio de Gedupeerde onderdeel was van BCO;

b) Of gegevens zijn opgenomen in CoronIT, HPZone Lite of beide systemen;

c) De categorieën persoonsgegevens die in de GGD-systemen zijn opgeslagen;

d) De duur dat persoonsgegevens in de GGD-systemen zijn opgeslagen; en

e) Of al dan niet vaststaat dat gegevens ongeoorloofd zijn ingezien en/of ontvreemd.

595. Dit betreft echter omstandigheden waarvan kan worden geabstraheerd. Beperkte feitelijke verschillen zijn inherent aan de afwikkeling van massaschade in collectieve acties en vormen geen belemmering voor het toepassen van de WAMCA. De rechtbank Den Haag oordeelde in dit kader in de zaak Milieuorganisaties/Shell:

> "4.2.4. De rechtbank is van oordeel dat het primair met de collectieve acties gediende belang van huidige en toekomstige generaties van de gehele wereldbevolking zich niet leent voor bundeling. Hoewel de hele wereldbevolking gediend is met het tegengaan van gevaarlijke klimaatverandering, zijn er grote verschillen in het moment en de manier waarop de wereldbevolking op de ene of de andere plaats getroffen zal worden door klimaatverandering als gevolg van CO2-emissies. Dit primaire belang voldoet dus niet aan het vereiste van 'gelijksoortig belang' van artikel 3:305a BW.
> Het subsidiair met de collectieve acties gediende belang van de huidige en de toekomstige generatie Nederlandse ingezetenen en (voor de Waddenvereniging) (de inwoners van) het deels in Nederland gelegen Waddengebied leent zich wel voor bundeling, ook al zijn er binnen Nederland en het Waddengebied verschillen in het moment, de mate en de intensiteit waarin de inwoners zullen worden getroffen door de klimaatverandering als gevolg van CO2-emissies. Deze verschillen zijn veel kleiner en van andere aard dan de onderlinge verschillen als het gaat om de hele wereldbevolking en staan niet in de weg aan bundeling in een collectieve actie."[286] (onderstreping door advocaat)

[285] Rechtbank Amsterdam, 30 juni 2021, ECLI:NL:RBAMS:2021:3307 (*Data Privacy Stichting/Facebook c.s.*), r.o. 7.11, 7.12 en 7.88.
[286] Rb Den Haag, 26 mei 2021, ECLI:NL:RBDHA:2021:5337, (*Milieuorganisaties/ Shell*) r.o. 4.2.4.

596. Voorgaande is ook door de rechtbank Amsterdam bevestigd in de aangehaalde uitspraak in de zaak Data Privacy Stichting/Facebook:

> "Voor zover de Stichting een oordeel vraagt over een of meer specifieke gebeurtenissen geldt dat de daarop betrekking hebbende vorderingen eveneens bundelbaar zijn. Ook daarbij is allereerst de vraag aan de orde of de betreffende gebeurtenis zich heeft voorgedaan en of de handelwijze van Facebook c.s. (on)rechtmatig is. In deze collectieve procedure hoeft nog niet te kunnen worden vastgesteld welke individuele belanghebbenden daardoor mogelijk zijn geraakt. Voldoende is dat op basis van het oordeel van de rechtbank een lid van de achterban kan vaststellen of hij is getroffen door een eventuele privacyschending. Op basis van de door de Stichting geformuleerde vorderingen zal dat moeten kunnen worden vastgesteld, nu in de beoordeling door de rechtbank zo nodig kan worden gedifferentieerd naar bijvoorbeeld wettelijk voorschrift, tijdsperiode en/of gebeurtenis."[287]

597. Ongeacht de concrete invulling van de genoemde feitelijke omstandigheden, geldt ten aanzien van ieder der Gedupeerden dat zij ten minste zijn blootgesteld aan een bepaalde ondergrens voor wat betreft de overtreding c.q. onrechtmatige handeling, welke ondergrens al van zodanige ernst en omvang is dat hun belang bij de bestrijding daarvan als gelijksoortig kan worden aangemerkt.

598. Voor zover toch geoordeeld zou worden dat verschillen in de omstandigheden sub a) tot en met d) tot de conclusie leiden dat de belangen van de Gedupeerden niet gelijksoortig zijn, geldt dat de belangen van ieder der Gedupeerden per afzonderlijke groep Gedupeerden zich evident voor bundeling lenen. Die verschillende groepen Gedupeerden zijn ook op zichzelf van voldoende omvang om een collectieve actie te rechtvaardigen.

599. Voor wat betreft de door Stichting ICAM ingestelde vordering tot collectieve schadevergoeding geldt dat deze, gelet op de nieuwe regels en waarborgen die de WAMCA biedt, moet worden geacht de effectieve en efficiënte rechtsbescherming van de Gedupeerden te bevorderen. De regering merkte hierover in de memorie van toelichting bij de WAMCA het volgende op:

> "Ten slotte is de procedure zelf zodanig vormgegeven dat het feit dat bepaalde bij een massaschade spelende vragen slechts individueel beantwoord kunnen worden, niet aan een efficiënte en effectieve afwikkeling in de weg behoeft te staan. […] De voorgestelde procedure kan worden ingezet voor de afwikkeling van alle soorten schade. Ook beperkt de procedure zich niet tot bepaalde vorderingsgerechtigden. [...]
> De voorgestelde procedure maakt geen onderscheid naar de oorzaak van de schade. […] Indien de rechter heeft geoordeeld dat de wederpartij onrechtmatig heeft gehandeld, kan de daardoor veroorzaakte massaschade in de voorgestelde procedure worden afgewikkeld."[288]

600. De regering heeft bij de invoering van de WAMCA expliciet het (in het verleden aangevoerde) bezwaar tegen collectieve schadevergoedingsacties, te weten dat causaliteit en schade slechts

[287] Rechtbank Amsterdam, 30 juni 2021, ECLI:NL:RBAMS:2021:3307 (*Data Privacy Stichting/Facebook c.s.*), r.o. 7.13.
[288] *Kamerstukken II* 2016-2017, 34 608, nr. 3, p. 7.

individueel kunnen worden bepaald, weggenomen door waarborgen in te bouwen die een efficiënte en effectieve afwikkeling van een collectieve schadevergoeding bevorderen. Die waarborgen zijn onder meer de aanvullende eisen die aan de professionaliteit van de belangenbehartiger worden gesteld, het aanwijzen van een Exclusieve Belangenbehartiger om duidelijkheid bij de gedaagden te creëren over de partij met wie eventueel kan worden onderhandeld over een schikking en de verschillende bevoegdheden van rechters om partijen te stimuleren tot een schikking te komen.[289] Duidelijk is dus dat de wetgever de WAMCA zo heeft ingericht dat mogelijke individuele factoren die bij de bepaling van de omvang van de schade in geval van onrechtmatig handelen een rol kunnen spelen, niet in de weg hoeven te staan aan een collectieve actie tot schadevergoeding.

601. Daar komt in de onderhavige zaak bij dat Stichting ICAM voor iedere Gedupeerde dezelfde forfaitaire schadevergoeding vordert (in twee categorieën) (paragraaf 5.3.2) en dat tussen het onrechtmatig handelen van de Staat c.s. en de door ieder der Gedupeerden geleden schade sprake is van dezelfde causaliteitsconstructie (paragraaf 6.2.5.3).

602. Dat ten aanzien van de hoogte van de schadevordering een onderscheid wordt gemaakt tussen Gedupeerden van wie is of zal worden vastgesteld dat gegevens ongeoorloofd zijn ingezien en/of ontvreemd enerzijds (Gedupeerden Categorie B) en Gedupeerden van wie niet is of zal worden vastgesteld dat gegevens ongeoorloofd zijn ingezien en/of ontvreemd anderzijds (Gedupeerden Categorie A) (omstandigheid sub e)), doet aan de gelijksoortigheid ook niet af.

603. Voorgaande wordt bevestigd in de memorie van toelichting bij de WAMCA[290] en in artikel 1018i lid 2 Rv:

> "2. De rechter stelt, mede aan de hand van de in het eerste lid bedoelde voorstellen, een collectieve schadeafwikkeling vast die strekt tot vergoeding door gedaagde van de schade van de in het eerste lid, onder a en b, bedoelde personen. De rechter draagt er zorg voor dat hij voor de toepassing van de tiende afdeling van de eerste titel van Boek 6 van het Burgerlijk Wetboek de schadevergoeding voor deze personen waar mogelijk in categorieën vaststelt, dat de collectieve schadeafwikkeling in ieder geval het in artikel 907, tweede lid, onderdelen a tot en met f, van Boek 7 van het Burgerlijk Wetboek bepaalde, bevat, dat de hoogte van de daarbij toegekende vergoedingen redelijk is en dat de belangen van de personen voor wie de collectieve schadeafwikkeling wordt vastgesteld ook anderszins voldoende gewaarborgd zijn. Artikel 907, eerste lid, laatste zin, en zesde lid, van Boek 7 van het Burgerlijk Wetboek zijn van overeenkomstige toepassing." [onderstreping advocaat]

604. De collectieve vorderingen die Stichting ICAM in deze zaak instelt bevorderen een efficiënte en effectieve rechtsbedeling. De schade die de Gedupeerden hebben geleden ten gevolge van het GGD-datalek is op individueel niveau relatief gering. Geen enkele Gedupeerde zal daarvoor naar

[289] *Kamerstukken II* 2016-2017, 34 608, nr. 3, p. 7.
[290] *Kamerstukken II* 2016/17, 34608, nr. 3, p. 52.

de rechter stappen. Het is onder meer om de vergoeding van dit soort “strooischade” mogelijk te maken dat de wetgever de collectieve schadevergoeding in het leven heeft geroepen.

9.1.2 Statuten en feitelijke werkzaamheden van Stichting ICAM

605. De behartiging van de belangen van de Gedupeerden in deze procedure valt binnen de statutaire doelomschrijving van Stichting ICAM. Artikel 3.1 van de Statuten omschrijft dat Stichting ICAM ten doel heeft om als onafhankelijke organisatie zonder winstoogmerk de belangen van gedupeerden te behartigen. In artikel 3.2 wordt dat doel nader gespecificeerd, waaronder ook valt het optreden tegen inbreuken op het recht op bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens, in het bijzonder inbreuken gepleegd door de overheid (**productie A.1**):

> “3.1 De Stichting stelt zich ten doel om als onafhankelijke organisatie en zonder winstoogmerk de belangen te behartigen van Gedupeerden, zijnde groepen natuurlijke personen, vennootschappen en/of rechtspersonen, in Nederland en/of daarbuiten, die zijn of dreigen te worden geraakt in een gelijksoortig belang in de zin van artikel 3:305a BW (of een vergelijkbare of daarvoor in de plaats tredende (wettelijke) regeling) en daardoor op enige derde(n) een of meer vordering(en) hebben verband houdend met door deze natuurlijke personen, vennootschappen en/of rechtspersonen geleden of te lijden Massaschade.
> 3.2 In het bijzonder valt onder het doel van de Stichting:
> a) Het optreden tegen (dreigende) inbreuken op het recht van burgers, consumenten, vennootschappen en/of rechtspersonen op bescherming van de persoonlijke levenssfeer en bescherming van persoonsgegevens, waaronder in het bijzonder tegen inbreuken door de overheid en/of overheidsinstanties, zoals de Staat en andere publiekrechtelijke rechtspersonen, waaronder begrepen het verhalen van Massaschade die deze Gedupeerden lijden en/of hebben geleden ten gevolge van inbreuken op genoemde rechten, waaronder begrepen overtredingen van de EU Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679) en/of enige daaruit voortvloeiende nationale wet- of regelgeving, beleidsregels, gedragscodes of normen;.’’

606. Artikel 3.3 van de Statuten noemt in dit verband verschillende relevante activiteiten om die doelstelling te bereiken. De vertegenwoordiging door Stichting ICAM in een collectieve procedure als de onderhavige en haar optreden namens de Gedupeerden in onder meer de media maakt deel uit van deze relevante activiteiten:

> “3.3 De Stichting tracht haar doel te bereiken met alle haar rechtens toekomende middelen, waaronder begrepen, zonder daartoe beperkt te zijn:
> a) Het in naam van de Stichting en/of in naam van de Gedupeerden starten en/of ondersteunen van juridische procedures, zoals civiele, strafrechtelijke of bestuursrechtelijke procedures, het instellen van (rechts)vorderingen of verzoeken, waaronder vorderingen of verzoeken tot het vergoeden, compenseren en/of ongedaan maken van Massaschade, het terugbetalen van onverschuldigd betaalde bedragen, het ongedaan maken van ongerechtvaardigde verrijking, het verkrijgen van verklaringen voor recht en het treffen van (voorlopige) voorzieningen, en het indienen van klachten bij

toezichthoudende instanties, een en ander in Nederland en in andere jurisdicties indien nodig en mogelijk, waaronder begrepen procedures, vorderingen, verzoeken en klachten (…);

b) Het (laten) doen van onderzoek naar (mogelijke) inbreuken op de rechten van Gedupeerden en naar de aansprakelijkheid van de (rechts)personen die (mogelijk) inbreuk maken of hebben gemaakt;

c) Het namens of in het belang van Gedupeerden voeren van onderhandelingen over en/of het aangaan van (collectieve) vaststellingsovereenkomsten, waaronder begrepen vaststellingsovereenkomsten in de zin van artikel 7:907 BW;

d) Het (laten) berekenen, vaststellen, verkrijgen, (door)betalen en distribueren van schadevergoedingen en het (laten) uitvoeren van (collectieve) vaststellingsovereenkomsten, waaronder begrepen vaststellingsovereenkomsten in de zin van artikel 7:907 BW;

e) Het optreden als woordvoerder en vertegenwoordiger van Gedupeerden, waaronder in de media, in de politiek, bij het bedrijfsleven, bij (potentiele) wederpartijen en in relatie tot het maatschappelijk middenveld;

f) Het informeren van Gedupeerden ten aanzien van zaken gerelateerd aan doel en werkzaamheden van de Stichting, onder meer via de Website;

g) Het beschikbaar stellen en/of door een externe partij beschikbaar latenstellen van adequate financiering voor het behalen van de doelstellingen van de Stichting, al dan niet tegen betaling van een financieringsvergoeding voor rente en gelopen risico;

h) Het bieden van de mogelijkheid aan Gedupeerden om Deelnemer te worden;

i) Het verrichten van al hetgeen met het vorenstaande in de ruimste zin verband houdt of daartoe bevorderlijk kan zijn.''

607. Stichting ICAM heeft onder meer de volgende activiteiten ondernomen:

a) Stichting ICAM heeft een website met informatie over de stichting (www.stichtingicam.nl) en een specifieke Website waarop zij het publiek informeert over deze collectieve actie (www.datalek-ggd.nl). Op de Website is ook informatie te vinden over Stichting ICAM, haar werkwijze en activiteiten. Geïnteresseerden kunnen via de Website vragen stellen en contact opnemen (**productie B.3 en B.4**);

b) De leden van de Raad van Bestuur en van de Raad van Toezicht van Stichting ICAM zijn allen al vele jaren op verschillende manieren (maatschappelijk) actief ter behartiging van de belangen die Stichting ICAM dient (paragraaf 2.1). Stichting ICAM is opgericht om de kwaliteiten en activiteiten van deze betrokken deskundigen te bundelen en in te zetten in het belang van door haar vertegenwoordigde personen, o.a. met betrekking tot het GGD-datalek;

c) Stichting ICAM publiceert regelmatig blogs en nieuwsartikelen die verband houden met het GGD-datalek en andere privacy-gerelateerde onderwerpen (**productie B.5**);

d) Stichting ICAM treedt in de media op met betrekking tot problemen en risico's rondom de beveiliging van persoonsgegevens en meer in het bijzonder, het GGD-datalek (**productie**

B.7). Zo was de woordvoerder van Stichting ICAM, Astrid Oosenbrug, te gast bij BNR Nieuwsradio om over de collectieve actie te vertellen en om aandacht te vragen voor dataveiligheid (**productie C.25**);

e) Stichting ICAM wordt door verschillende privacy-organisaties gesteund in het voeren van deze collectieve procedure en is met hen in overleg over de vraag of zij hun steun publiekelijk bekend willen maken;

f) Stichting ICAM heeft onderzoek gedaan en doet nog steeds onderzoek naar de verwerking en beveiliging van persoonsgegevens in verband met het GGD-datalek, en de maatregelen die de Staat c.s. hebben genomen om het GGD-datalek en (verdere) schade van de Gedupeerden te voorkomen. Onder andere heeft Stichting ICAM meer dan 75 Woo-verzoeken gedaan om in dit kader meer informatie te achterhalen en heeft zij naar aanleiding daarvan bezwaar gemaakt tegen vier Woo-besluiten (paragraaf 1.5);

g) Stichting ICAM heeft onderzoek gedaan naar de verschillende strafzaken naar aanleiding van het GGD-datalek en is daartoe in contact geweest met het OM, de rechtbanken en de behandelende strafadvocaten;

h) Stichting ICAM is in contact geweest met ethische hackers en met cybercriminelen om bevestigd te krijgen dat inderdaad grote databestanden met persoonsgegevens uit het GGD-datalek worden aangeboden in het criminele circuit;

i) Stichting ICAM werkt samen met verschillende journalisten die onderzoek doen naar het GGD-datalek, in het bijzonder naar de onzorgvuldigheid in de aanloop daarnaartoe;

j) Stichting ICAM heeft onderhandelingen gevoerd met verschillende financiers om de onderhavige procedure te bekostigen, zodat de belangen van de Gedupeerden behoorlijk kunnen worden vertegenwoordigd;

k) Stichting ICAM heeft de Staat c.s. in een uitgebreide brief aansprakelijk gesteld voor de schade die de Gedupeerden hebben geleden als gevolg van het GGD-datalek;

l) Stichting ICAM heeft overleg gevoerd met Gedaagden in een poging om buiten rechte tot een oplossing te komen. In dat kader hebben meerdere besprekingen plaatsgevonden en is uitgebreid schriftelijk gecommuniceerd (paragraaf 1.4 en 9.1.4.3);

m) Stichting ICAM is continu opmerkzaam op andere mogelijke collectieve acties binnen haar statutaire doelstellingen, heeft een aantal mogelijke acties al verder onderzocht en heeft in dat kader reeds mogelijkheden voor procesfinanciering onderzocht. Momenteel is één concrete collectieve actie in een vergevorderd stadium van vooronderzoek. Dit betreft een kartelschadezaak ten behoeve van een grote groep consumenten;

n) Stichting ICAM heeft een flyer gemaakt om haar doelstellingen en activiteiten onder de aandacht te brengen van advocaten, financiers en gedupeerden (**productie B.13**).

9.1.3 Waarborgvereiste

608. Artikel 3:305a lid 1 BW bepaalt dat de belangen van degenen waarvoor de belangenorganisatie opkomt voldoende dienen te zijn gewaarborgd. Artikel 3:305a lid 2 BW bepaalt dat dit het geval is indien de belangenorganisatie voldoende representatief is, gelet op de achterban en de omvang van de vertegenwoordigde vorderingen en beschikt over:

a) Een toezichthoudend orgaan (behoudens enkele uitzonderingen die in onderhavige zaak niet van toepassing zijn);

b) Een passend en doeltreffend mechanisme voor deelname aan of vertegenwoordiging bij de besluitvorming van de vertegenwoordigde personen;

c) Voldoende middelen om de kosten voor het instellen van de vordering te dragen, waarbij de zeggenschap over de vordering in voldoende mate bij de rechtspersoon moet liggen;

d) Een algemeen toegankelijke internetpagina, waarop bepaalde informatie beschikbaar moet zijn; en

e) Voldoende ervaring en deskundigheid ten aanzien van het instellen en voeren van de rechtsvordering.

609. Stichting ICAM zal in de volgende paragrafen toelichten dat zij aan al deze waarborgeisen voldoet.

9.1.3.1 Representativiteit

610. Stichting ICAM is representatief voor de groep Gedupeerden die zij vertegenwoordigt in deze collectieve actie. Het representativiteitsvereiste dient ertoe te voorkomen dat een rechtspersoon een vordering in kan stellen zonder dat zij een achterban vertegenwoordigt die gebaat is bij de uitkomst van de procedure. Of een belangenorganisatie voldoende representatief is, kan uit verschillende gegevens worden afgeleid. Een vastomlijnde invulling van dit begrip is er niet, omdat dit tekort zou doen aan andere omstandigheden die er eveneens op kunnen wijzen dat een belangenorganisatie representatief is.

611. Indicaties voor representativiteit zijn bijvoorbeeld de vraag in hoeverre de gedupeerden de organisatie zelf als representatief ervaren, de expertise en ervaring van de organisatie, de overige werkzaamheden die de organisatie verricht heeft, het aantal aangesloten gedupeerden en de

omvang van hun vorderingen ten opzichte van het totaal aantal gedupeerden van een massagebeurtenis en de door hen gevorderde schadevergoeding.[291]

612. Op voorhand moet duidelijk zijn dat de belangenorganisatie kwantitatief gezien voor een voldoende groot deel van de groep getroffen gedupeerden opkomt. Welk aantal genoeg is, verschilt per geval, maar kan bijvoorbeeld worden getoetst door middel van het aantal gedupeerden dat zich actief voor de collectieve actie heeft aangemeld.[292] Voldoende is dat nauwkeurig wordt omschreven voor welke groep van personen de belangenorganisatie opkomt.

613. Stichting ICAM komt in deze procedure op de voet van artikel 3:305a BW op voor alle Gedupeerden, dat wil zeggen alle natuurlijke personen van wie persoonsgegevens zijn verwerkt in één van of beide GGD-systemen in de periode tussen ingebruikname daarvan in verband met de bestrijding van corona en 1 februari 2021, bijvoorbeeld omdat zij een afspraak hebben gemaakt bij een GGD om te testen of vaccineren in verband met corona of omdat zij onderdeel zijn geweest van bron- en contactonderzoek in verband met corona. Van al deze personen staat immers vast dat:

a) Hun gegevens opgenomen zijn of opgenomen zijn geweest in CoronIT en/of HPZone Lite gedurende een periode waarin de beveiliging van die systemen niet op orde was;

b) Er dus een risico bestaat dat hun gegevens ongeautoriseerd zijn ingezien en mogelijk zijn gestolen; en

c) Zij dus de controle over hun persoonsgegevens kwijt zijn.

614. De groep Gedupeerden bestond op het moment van de berichtgeving door RTL Nieuws in januari 2021 uit ongeveer 6,5 miljoen mensen (paragraaf 3.4).

615. De Gedupeerden kunnen worden onderverdeeld in twee subgroepen:

a) **Gedupeerden Categorie A**: Alle Gedupeerden, met uitzondering van de personen die deel uitmaken van Gedupeerden Categorie B;

b) **Gedupeerden Categorie Groep B**: Alle Gedupeerden waarvan vaststaat of zal worden vastgesteld dat hun persoonsgegevens als gevolg van het GGD-datalek door ongeautoriseerde personen zijn ingezien of bij ongeautoriseerde personen in handen zijn gekomen, zoals door het ongeoorloofd inzien, downloaden, exporteren, printen, kopiëren, fotograferen en/of, aanbieden, verhandelen, ontvangen of op andere wijze delen van de persoonsgegevens.

[291] *Kamerstukken II* 2016/17, 34608, 3, p. 18 en 19.
[292] *Kamerstukken II* 2016/17, 34608, 3, p. 19.

616. Volgens de Staat c.s. heeft de politie vastgesteld dat gegevens van ongeveer 1.250 personen zijn ontvreemd (Gedupeerden Categorie B, paragraaf 3.4). Naar overtuiging van Stichting ICAM is deze groep echter (veel) groter, van welke stelling zij bewijs aanbiedt (hoofdstuk 8).

617. GGD GHOR heeft de groep van 1.250 personen tegen finale kwijting een aanbod gedaan van € 500,- om de zaak te schikken (paragraaf 3.1.12). Volgens GGD GHOR heeft ongeveer 70% van deze groep dat aanbod geaccepteerd (**productie H.2M**). Dat betekent echter niet dat Stichting ICAM geen vorderingen meer kan instellen namens deze groep. De formulering van de finale kwijting in de brief van GGD GHOR luidt namelijk als volgt (paragraaf 3.1.12):

> "Dit betekent dat u ermee akkoord gaat dat wij tegenover u geen verplichtingen meer hebben die te maken hebben met de datadiefstal uit de coronasystemen van de GGD. Dit geldt dan voor verplichtingen van GGD GHOR Nederland, de GGD'en of andere overheidsinstanties (zoals de gemeente of de landelijke overheid"

618. De finale kwijting ziet dus uitsluitend op schade in verband met "de datadiefstal". In de brief wordt "de datadiefstal" omschreven als "de foto's (schermafdrukken) van gegevens in CoronIT" (**productie H.2M**). De brief rept niet over het risico dat gegevens op andere wijze zijn gestolen uit CoronIT of dat ook gegevens zijn gestolen uit HPZone Lite. De finale kwijting ziet dus niet op eventuele schade die deze Gedupeerden hebben geleden ten gevolge van die risico's of de eventuele verwezenlijking daarvan.

619. Tussen 6 december 2021 en de datum van deze Dagvaarding hebben 133.691 personen zich voor deze collectieve actie bij Stichting ICAM aangemeld. Hoewel dat vanwege de totale omvang van de groep percentueel een klein aantal is, is het in absolute zin een ongekend hoog aantal actief aangeslotenen voor een collectieve actie. Stichting ICAM is dan ook van mening dat zij enkel vanwege dit absolute aantal reeds als representatief dient te worden gezien. Stichting ICAM vraagt nog steeds actief aandacht voor deze collectieve actie en deze komt ook nog regelmatig in het nieuws. Te verwachten is dan ook dat zich na dagvaarding nog veel meer Deelnemers zullen aansluiten. Alle Deelnemers vallen binnen de groep Gedupeerden. Stichting ICAM heeft dit vastgesteld door in het aanmeldformulier te vragen of zij een test- of vaccinatieafspraak hebben gemaakt of zijn benaderd voor bron- en contactonderzoek (**productie B.3**). Stichting ICAM heeft daarnaast NAW- en contactgegevens van de Deelnemers verzameld om hen, hoewel niet vereist, te kunnen identificeren.

620. De feitelijke werkzaamheden van Stichting ICAM zijn hiervoor in paragraaf beschreven. Daaruit blijkt dat Stichting ICAM zich daadwerkelijk actief inzet voor de Gedupeerden.

621. Stichting ICAM beschikt bovendien over voldoende expertise en ervaring om de belangen van de Gedupeerden te behartigen (paragraaf 9.1.3.6), hetgeen ook als indicatie dient te gelden dat zij voldoende representatief is.[293]

9.1.3.2 Raad van Toezicht

622. Stichting ICAM beschikt over een toezichthoudend orgaan, namelijk een Raad van Toezicht. De Raad van Toezicht heeft op grond van de Statuten adequate bevoegdheden en waarborgen om haar toezichthoudende taak onafhankelijk en kritisch uit te voeren:

a) De leden van de Raad van Toezicht worden benoemd, geschorst en ontslagen door de Raad van toezicht zelf (artikel 13.4);

b) De Raad van Toezicht heeft tot taak toezicht te houden op het beleid en de strategie van de Raad van Bestuur en op de algemene gang van zaken in de stichting. Bij de vervulling van hun taken richten de leden van de Raad van Toezicht zich naar het belang van de stichting en de met haar verbonden organisatie (artikel 14.1);

c) De Raad van Bestuur dient de Raad van Toezicht tijdig de nodige informatie te verschaffen voor de uitvoering van zijn taken en bevoegdheden, waaronder begrepen maar niet beperkt tot de notulen van de vergaderingen van het Bestuur. Voorts dient de Raad van Bestuur desgevraagd elk lid van de Raad van Toezicht alle informatie te verschaffen die betrekking heeft op de aangelegenheden van de Stichting (artikel 14.2);

d) De Raad van Toezicht is bevoegd inzage te nemen in de boeken, bescheiden en andere gegevensdragers van de stichting (artikel 14.3);

e) Ieder lid van de Raad van Toezicht heeft toegang tot alle gebouwen en gronden in gebruik bij de stichting (artikel 14.4);

f) De Raad van Toezicht kan zich bij de uitoefening van zijn taak voor rekening van de stichting laten bijstaan door deskundigen (artikel 14.5);

g) Ten minste eenmaal per jaar wordt een gemeenschappelijke vergadering van de Raad van Bestuur en de Raad van Toezicht gehouden (artikel 17.1) en voorts zo vaak als een lid van de Raad van Toezicht dat wenselijk acht (artikel 17.2);

h) De Raad van Toezicht benoemt, schorst en ontslaat de leden van de Raad van Bestuur (artikel 6.4);

[293] *Kamerstukken II* 2003/04, 29414, 3, p. 15.

i) De Raad van Bestuur dient ten minste één keer per jaar verantwoording af te leggen aan de Raad van Toezicht over de vaststelling en uitvoering van het (financieel) beleid en de op verwezenlijking van de statutaire doelstelling gerichte strategie (artikel 7.3);

j) De Raad van Bestuur is verplicht om elke voorgenomen substantiële wijziging in de governancestructuur van de stichting en in de naleving van de Claimcode ter bespreking voor te leggen aan de Raad van Toezicht (artikel 7.4);

k) Aan de goedkeuring van de Raad van Toezicht zijn onderworpen besluiten van de Raad van Bestuur omtrent wijziging van de Statuten, fusie of splitsing, ontbinding, het aanhangig maken van een gerechtelijke procedure, het sluiten van een schikkingsovereenkomst, het aangaan of beëindigen van enige financieringsovereenkomst en het vaststellen of wijzigen van de jaarlijkse begroting (artikel 9.10, 22.2, 22.7, 23.2 en 24.2). De Raad van Toezicht kan bovendien andere besluiten van de Raad van Bestuur aan zijn goedkeuring onderwerpen (artikel 9.11);

l) De Raad van Toezicht mag, voordat hij goedkeuring verleent aan de balans en de staat van baten en lasten zoals opgesteld door de Raad van Bestuur, deze stukken laten onderzoeken door een registeraccountant of een andere deskundige (artikel 22.5); en

m) De Raad van Toezicht stelt onkostenvergoeding, vacatiegeld en honorarium voor de leden van de Raad van Bestuur vast (artikel 10.2).

623. De Raad van Toezicht handelt onafhankelijk en kritisch ten opzichte van de Raad van Bestuur en ten aanzien van de door Stichting ICAM behartigde belangen, zoals ook vastgelegd in artikel 13.2 en artikel 18 van de Statuten.

624. De Raad van Toezicht stelt op grond van artikel 14.6 van de Statuten jaarlijks een document op waarin hij op hoofdlijnen verantwoording aflegt over het door hem uitgevoerde toezicht. Dit document wordt op de Website geplaatst. Het eerste verantwoordingsdocument van de Raad van Toezicht dateert van 14 juli 2022 en is gepubliceerd op de Website (**productie B.3** en **productie B.9**).

9.1.3.3 Mechanisme voor deelname aan of vertegenwoordiging bij de besluitvorming

625. Op grond van artikel 3:305a BW lid 2 sub b BW moet een belangenorganisatie over doeltreffende en passende mechanismen beschikken voor de deelname aan of vertegenwoordiging bij de besluitvorming van de personen voor wie de rechtsvordering is ingesteld. Belangenorganisaties zijn vrij om te bepalen op welke manier zij hieraan invulling geven. In dit verband geldt dat wanneer een belangenorganisatie is ingericht overeenkomstig de Claimcode 2019, kan worden

aangenomen dat is voldaan aan dit vereiste.[294] Stichting ICAM zal in paragraaf 9.1.3.7 toelichten dat zij voldoet aan de Claimcode 2019.

626. Stichting ICAM is bovendien voornemens, en heeft al aangekondigd (**productie B.6**), dat zij de Deelnemers door middel van een videobijeenkomst zal bijpraten over de zaak en zal vragen naar hun reactie en inbreng. Indien Stichting ICAM op enig moment een schikking met de Staat c.s. overweegt, dan zal zij de Deelnemers daarover informeren. Op welke wijze dat zal gebeuren en op welke wijze Stichting ICAM daarbij de inbreng van de Deelnemers zal verzamelen en meewegen, zal Stichting ICAM bepalen aan de hand van de voorliggende schikking en de stand van zaken op dat moment.

9.1.3.4 Financiële middelen en zeggenschap

627. Artikel 3:305a lid 2 sub c BW stelt de eis dat de belangenorganisatie over voldoende financiële middelen beschikt om de collectieve vordering in te stellen, waarbij de zeggenschap over de vordering in voldoende mate bij de belangenorganisatie moet blijven liggen. Voldoende is dat de belangenbehartiger kan aangeven dat hij, op het moment van toetsing, over voldoende middelen beschikt of kan beschikken om de procedure te kunnen voeren.[295] De toetsing is marginaal. Niet nodig is dat de wederpartij inzage in de financieringsovereenkomst krijgt.[296]

628. Stichting ICAM heeft op 7 december 2021 een Financieringsovereenkomst gesloten met Liesker Procesfinanciering B.V. te Breda (zie randnummers 653 e.v.). In die Financieringsovereenkomst heeft de Financier toegezegd de volledige kosten van de collectieve actie te financieren, waaronder de proceskosten voor de volledige procedure in eerste aanleg en de kosten voor het incasseren en verdelen van toegewezen schadevergoedingen. Stichting ICAM beschikt aldus over voldoende middelen om deze collectieve vordering in te stellen.

629. In die Financieringsovereenkomst is bepaald dat Stichting ICAM volledig verantwoordelijk is en blijft voor de uitvoering van de collectieve actie en de volledige zeggenschap heeft over de actie en alle aspecten van haar activiteiten, waaronder de proces- en schikkingsstrategie en de inschakeling van dienstverleners en/of andere derden dan wel de beëindiging van de relatie daarmee.

630. Stichting ICAM zal bij de bespreking van Principe III van de Claimcode de externe financiering in meer detail toelichten (randnummers 653 e.v.) en verzoekt hetgeen daar is opgenomen als hier herhaald en ingelast te beschouwen.

---

294 *Kamerstukken II* 2016/17, 34608, 3, p. 20.
295 *Kamerstukken II* 2016/17, 34608, 3, p. 11/12 en 20.
296 HR 20 december 2002, ECLI:NL:PHR:2002:AE3350 (*Lightning Casino/Antillen*); *Kamerstukken II* 2017/18, 34608, 6, p. 11 - 12.

9.1.3.5 Algemeen toegankelijke website

631. Artikel 3:305a lid 2 sub d BW vereist dat een belangenorganisatie over een algemeen toegankelijke internetpagina beschikt.

632. Stichting ICAM beschikt over een website met informatie over de stichting (www.stichtingicam.nl) en een specifieke Website waarop zij het publiek informeert over deze collectieve actie (www.datalek-ggd.nl). Op de Website is alle documenten en informatie te vinden die wordt voorgeschreven door artikel 3:305a lid 2 sub d BW, waaronder:

a) De Statuten (**productie B.1**);

b) De Claimcode 2019 (**productie B.2**);

c) Een Verantwoordingsdocument Wet en Claimcode (**productie B.8**);

d) De Deelnemersovereenkomst (**productie B.11 en B.12**);

e) De bestuursstructuur van de stichting (**productie B.3 en B.4**);

f) De laatst vastgestelde jaarlijkse verantwoording van de Raad van Toezicht d.d. 14 juli 2022 (**productie B.9**);

g) Het laatst vastgestelde bestuursverslag d.d. 14 juli 2022 (**productie B.10**);

h) Informatie over de bezoldiging van de leden van de Raad van Bestuur en de Raad van Toezicht (**productie B.3 en B.8**);

i) De doelstellingen en werkwijzen van Stichting ICAM (**productie B.3 en B.4**);

j) Een overzicht van de stand van zaken in de lopende procedure (**productie B.3**);

k) Informatie over de berekening van de no cure, no pay-vergoeding (**productie B.3, B.8, B.11 en B.12**); en

l) Informatie over de wijze waarop Gedupeerden zich kunnen aansluiten en deze aansluiting kunnen beëindigen (**productie B.3, B.11 en B.12**).

9.1.3.6 Ervaring en deskundigheid

633. Artikel 3:305a lid 2 sub e BW vereist ten slotte dat de leden van de Raad van Bestuur en de Raad van Toezicht beschikken over voldoende ervaring en expertise die noodzakelijk is voor het instellen van de collectieve actie.

634. De leden van de Raad van Bestuur en Raad van Toezicht van Stichting ICAM beschikken over ruime en relevante juridische ervaring en expertise, waaronder op het gebied van collectieve acties en gegevensbescherming, over kennis van ICT en over de benodigde financiële expertise en ervaring. Daarnaast maakt Stichting ICAM gebruik van een team van gespecialiseerde advocaten met ruime ervaring in collectieve acties, gegevensbeschermingsrecht en ICT.

Raad van Bestuur

635. De Raad van Bestuur bestaat uit de heer Marnix Bos, de heer Tijs Breukink en mevrouw Astrid Oosenbrug.

636. Marnix Bos is de voorzitter van de Raad van Bestuur. De heer Bos is advocaat, momenteel als partner verbonden aan Berculo Advocaten in Utrecht. Daarvoor werkte hij tien jaar als advocaat bij AKD Prinsen Van Wijmen in Rotterdam en Utrecht. Naast zijn werk als advocaat is Bos sinds 2017 voorzitter van de Stichting Wakkerpolis, een organisatie die met succes collectieve acties tegen grote verzekeraars voert over woekerpolissen. In een einduitspraak van de procedure die Stichting Wakkerpolis sinds 2017 namens circa 600.000 polishouders voerde tegen Nationale-Nederlanden, oordeelde de Rechtbank Rotterdam op 20 juli 2022 dat Nationale-Nederlanden jarenlang “eerste kosten” in rekening had gebracht bij beleggingsverzekeringen zonder dat dit was overeengekomen. De uitspraak betekent volgens berekeningen van Stichting Wakkerpolis een te vergoeden schade van ten minste € 350 miljoen. De raad van toezicht van Stichting Wakkerpolis bestaat uit de heer [redacted], de heer [redacted] en voormalig raadsheer bij de Hoge Raad, de heer mr. [redacted]. Professor mr. [redacted] zit in de adviesraad van Stichting Wakkerpolis. De heer Bos heeft dan ook veel relevante werkervaring op het gebied van collectieve acties en in het besturen van 3:305a-belangenorganisaties.

637. Tijs Breukink is specialist bedrijfskunde en bedrijfseconomie en een zeer ervaren bestuurder op de portefeuille financiën. De heer Breukink studeerde bedrijfseconomie en promoveerde ook op dit vakgebied. Hij heeft tot 2005 diverse managementfuncties gehad in het bedrijfsleven, onder meer bij Arcadis en DAF Trucks. Op dit moment is de heer Breukink interim-directeur bij de Faculty of Behavioral, Management and Social Sciences van de Universiteit van Twente. Daarvoor heeft hij diverse andere (interim-)bestuursfuncties vervuld. Zo was hij van 2005 tot 2017 lid van de raad van bestuur van Wageningen University & Research. Na 2017 is hij onder meer interim-lid van de raad van bestuur van de Hogeschool Arnhem-Nijmegen geweest. Breukink beschikt derhalve over de benodigde financiële expertise en ervaring om verantwoordelijkheid te nemen voor het financiële beleid van Stichting ICAM.

638. Astrid Oosenbrug is oud-Tweede Kamerlid en een ervaren bestuurder. In haar Kamerwerk was ICT en dataveiligheid haar belangrijkste speerpunt. Zo was zij van 2012 tot en met 2017 woordvoerder op het gebied van overheidsdienstverlening, ICT en data bij de overheid, privacy en telecommunicatie en auteursrecht. Gedurende haar Kamerlidmaatschap heeft mevrouw Oosenbrug zich onder meer sterk gemaakt voor de invoering van het Responsible Disclosure-beleid binnen de Nederlandse overheid. Oosenbrug heeft verder ervaring als IT-

systeembeheerder bij onder andere XS4all, Stichting IT-works! en Omroep West. Momenteel is zij Public Affairs Officer bij ESET, een bekend IT-beveiligingsbedrijf, voorzitster van het Dutch Institute for Vulnerability Disclosure, een organisatie die zich richt op het onderzoeken en rapporteren van IT-beveiligingsgebreken en cyber security incidenten, en voorzitster van het COC, een landelijke lhbti-belangenorganisatie. Mevrouw Oosenbrug heeft tijdens de coronapandemie als vrijwilliger voor de GGD (via de ANWB) bron- en contactonderzoek uitgevoerd.

639. De Raad van Bestuur wordt bijgestaan door de heer Adriaan de Gier, die op grond van een opdrachtovereenkomst als operationeel manager verantwoordelijk is voor de dagelijkse gang van zaken van Stichting ICAM. De heer De Gier heeft in het kader van deze collectieve actie onder andere contact met de advocaten, de Financier en de Raad van Bestuur en Raad van Toezicht. De Gier is gespecialiseerd in het aansprakelijkheidsrecht, waaronder in het bijzonder collectieve acties, als advocaat maar ook als bestuurslid. Zo is hij als advocaat van Stichting FortisEffect vanaf het begin nauw betrokken geweest bij de collectieve procedure over beleggersmisleiding in de aanloop naar het ontmantelde Fortis (nu Ageas) in 2008,[297] bij de totstandkoming van de schikking van die zaak ter grootte van € 1,3 miljard en bij de afwikkeling daarvan op basis van de verbindendverklaring van die schikking door het gerechtshof Amsterdam op basis van de WCAM.[298] Ook is hij als advocaat betrokken bij de collectieve zaken van Stichting Wakkerpolis tegen NN en ASR inzake beleggingsverzekeringen, tegen Airbnb (als adviseur) en tegen Achmea Bank (Staalbankiers) (als voorzitter van het bestuur van de Stichting Compensatie Zwitserse Frank Leningen CZFL).

Raad van Toezicht

640. De Raad van Toezicht bestaat momenteel uit mevrouw Quirine Eijkman en de heer Rob van den Hoven van Genderen. De heer [redacted], die als lid van de Raad van Toezicht was voorgedragen door de Financier, is helaas op 21 juni 2022 onverwacht overleden. Er wordt op dit moment gezocht naar geschikte vervanging met financiële expertise. De verwachting is dat op korte termijn een nieuw lid zal worden benoemd.

641. Quirine Eijkman is voorzitster van de Raad van Toezicht. Mevrouw Eijkman is lector Toegang tot het Recht bij de Hogeschool Utrecht en ondervoorzitter bij het College voor de Rechten van de Mens. In haar werk richt Eijkman zich op maatschappelijke vraagstukken die verband houden met de toegang tot het recht, veiligheid, digitalisering, herstelrecht en mensenrechten. Zo zit mevrouw Eijkman in de Raden van Advies van de Raad voor de Rechtsbijstand, het Nederlands Juristen Comité voor de Mensenrechten (NJCM) en de Stichting Privacy First. Ook is mevrouw

[297] Uitgemond in veroordeling van Fortis tot betaling van schadevergoeding door het gerechtshof te Amsterdam in 2014: ECLI:NL:GHAMS:2014:3005.
[298] ECLI:NL:GHAMS:2018:2422.

Eijkman lid van de Commissie Werkelijke Schade en de Kenniskring van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).

642. Rob van den Hoven van Genderen is directeur van het Centrum voor Recht en Internet (CLI) van de Vrije Universiteit Amsterdam, hoogleraar AI & Robotlaw aan de University of Lapland en visiting professor bij de Kyushu University in Japan en de nationale universiteit van Taiwan (NTU). Als universitair docent geeft Van den Hoven van Genderen onder meer colleges over privacyrecht, internetrecht en AI. Over deze onderwerpen publiceerde hij verschillende boeken en artikelen. In het verleden was de heer Van den Hoven van Genderen speciaal adviseur voor de VN en de Raad van Europa over privacy. Naast zijn huidige wetenschappelijke werk is hij consulting partner van SwitchLegal International Lawyers en redactielid van het tijdschrift Computerrecht.

9.1.3.7 Stichting ICAM voldoet aan de Claimcode

643. Stichting ICAM onderschrijft de principes uit de Claimcode 2019 en houdt zich daaraan zoals beschreven in het Verantwoordingsdocument dat ieder jaar beschikbaar wordt gesteld op de Website (**productie B.8**). De manier waarop Stichting ICAM invulling geeft aan de principes uit de Claimcode 2019 wordt hieronder nader uiteengezet.

Principe I – Naleving en handhaving van de code

644. De Statuten bepalen in artikel 3.5 dat Stichting ICAM haar statuten, organisatie en werkwijze zoveel mogelijk inricht conform de uitgangspunten van de Claimcode 2019. De Raad van Bestuur en de Raad van Toezicht zijn verantwoordelijk voor naleving van de Claimcode 2019 en de governancestructuur. De hoofdlijnen van de governancestructuur van Stichting ICAM zijn beschreven in het Verantwoordingsdocument, de Statuten en op de Website (**producties B.1, B.3, B.4 en B.8**). In het Verantwoordingsdocument wordt toegelicht op welke wijze de Claimcode 2019 wordt opgevolgd en waar daarvan wordt afgeweken, waarom, dit volgens het 'pas toe of leg uit'-principe uit de Claimcode 2019. Deze informatie blijft beschikbaar zolang Stichting ICAM actief is. Voorgaande is ook vastgelegd in artikel 20 van de Statuten.

645. In artikel 7.4 van de Statuten is voorts vastgelegd dat de Raad van Bestuur verplicht is om iedere voorgenomen wijziging in de governancestructuur en in de nalevering van de Claimcode 2019 ter bespreking voor te leggen aan de Raad van Toezicht.

Principe II – Stichting ICAM heeft geen winstoogmerk

646. Stichting ICAM heeft geen winstoogmerk. Dit is vastgelegd in artikel 3.4 van de Statuten. Dat Stichting ICAM geen winstoogmerk heeft volgt ook uit haar doelstellingen en feitelijke werkzaamheden.

647. Uitsluitend indien in deze procedure of in een schikking een schadevergoeding wordt toegekend of overeengekomen, maakt Stichting ICAM aanspraak op een no cure, no pay-vergoeding. Die vergoeding wordt uitsluitend gebruikt ter dekking van de door Stichting ICAM gemaakte kosten in verband met haar juridische en administratieve dienstverlening, de financiering van die kosten en de daaraan verbonden risico's. Kort gezegd wordt de no cure, no pay-vergoeding uitsluitend gebruikt om de Financier terug te betalen, inclusief de met de Financier overeengekomen vergoeding voor het financieringsrisico (zoals verder toegelicht bij de behandeling van Principe III hieronder).

648. De met de Financier overeengekomen vergoeding voor het dragen van de kosten van deze procedure is redelijk en strookt met Principe II.2 en Principe III van de Claimcode 2019. De afspraak houdt in dat als in een niet-aantastbare einduitspraak schadevergoeding wordt toegewezen of in een schikking wordt overeengekomen, de Financier een vergoeding ontvangt ter hoogte van (i) de reëel gemaakte kosten (proceskosten, buitengerechtelijke kosten en/of financieringskosten) vermeerderd met (ii) een vergoeding voor rente en risico ter hoogte van 20% van het aan de Gedupeerden toegekende bedrag. De onder (ii) bedoelde vergoeding voor de Financier is echter gemaximeerd op vijfmaal de door haar in de collectieve actie geïnvesteerde som, zodat exorbitante financieringsvergoedingen worden voorkomen. Deze afspraak is neergelegd in artikel 7 van de Financieringsovereenkomst.

649. Stichting ICAM vordert om de Staat c.s. te veroordelen de no cure, no pay-vergoeding te betalen (paragraaf 11.7 en vordering O). Uitsluitend indien door de rechtbank wel een schadevergoeding wordt toegewezen maar de no cure, no pay-vordering wordt afgewezen of indien de no cure, no pay-vergoeding geen onderdeel uitmaakt van een eventuele schikking, zijn de Deelnemers de no cure, no pay-vergoeding aan Stichting ICAM verschuldigd. De no cure, no pay-vergoeding bedraagt dan maximaal 20% van het toegewezen bedrag aan schade. Dit is vastgelegd in de Deelnemersovereenkomst en het Verantwoordingsdocument (**producties B.8, B.11 en B.12**).

650. Indien de totale aan Stichting ICAM toekomende no cure, no-pay-vergoeding het bedrag overstijgt dat Stichting ICAM aan kosten heeft gemaakt (waaronder financieringskosten, zoals conform de Financieringsovereenkomst verschuldigd aan de Financier), dan zal 10% van dat overschot ten goede komen aan Stichting ICAM voor toekomstige collectieve belangenbehartiging op het gebied van massaschade, met een maximum van € 150.000,-. Het restant van een eventueel overschot zal naar rato worden verdeeld onder alle Gedupeerden van het GGD-datalek, waarbij eerst de Deelnemers zullen worden gecompenseerd voor de eventueel door hen betaalde no cure, no pay-vergoeding. Deze regeling is in overeenstemming met uitwerking 2 van Principe II van de Claimcode en is vastgelegd in de Deelnemersovereenkomst en het Verantwoordingsdocument (**producties B.8, B.11 en B.12**).

651. In overeenstemming met de uitwerking van Principe II van de Claimcode 2019 is voorts in artikel 5.3 van de Statuten vastgelegd dat een natuurlijke persoon noch een rechtspersoon, geheel of gedeeltelijk, over het vermogen en de inkomsten van Stichting ICAM kan beschikken als ware het

zijn of haar eigen vermogen en inkomsten. Verder is in artikel 8.1 van de Statuten opgenomen dat alleen twee bestuurders gezamenlijk bevoegd zijn om Stichting ICAM te vertegenwoordigen.

652. Verder is in artikel 24.3 van de Statuten bepaald dat de bestemming van een eventueel batig liquidatiesaldo zoveel mogelijk in overeenstemming met het doel van Stichting ICAM ten goede zal komen aan haar Deelnemers, dan wel aan een geschikte goede-doelenorganisatie.

Principe III – Externe financiering

653. Stichting ICAM heeft externe financiering aangetrokken om deze collectieve actie te bekostigen, zodat de Gedupeerden de collectieve actie niet hoeven voor te financieren en geen proceskostenrisico lopen.

654. De Financier betreft Liesker Procesfinanciering B.V. uit Breda. Liesker Procesfinanciering is een bekende en gerenommeerde Nederlandse procesfinancier. Sinds haar oprichting in 2011 heeft zij vele zaken gefinancierd, waaronder collectieve acties. De onderneming is opgericht vanuit de idealistische gedachte en de ervaring dat veel belangrijke en kansrijke zaken nooit worden gevoerd omdat de schadelijdende partij onvoldoende financiële middelen heeft of tegenover een veel grotere wederpartij staat. Liesker Procesfinanciering biedt rechtszoekenden de garantie dat wanneer zij een zaak aanneemt, zij de procedure van begin tot eind zal financieren. Liesker Procesfinanciering staat erom bekend ethiek hoog in het vaandel te hebben staan, waarbij haar overtuiging is dat procesfinanciering ervoor zorgt dat het rechtssysteem voor iedereen toegankelijk is en een ieder gelijke kansen biedt.

655. Stichting ICAM heeft op 7 december 2021 een Financieringsovereenkomst gesloten met de Financier. In die Financieringsovereenkomst heeft de Financier toegezegd de volledige kosten van de collectieve actie te financieren, waaronder (zonder daartoe beperkt te zijn) de kosten voor overleg met de Gedaagden, de buitengerechtelijke kosten en proceskosten voor de volledige procedure in eerste aanleg (inclusief incidenten en eventuele hoger beroepen van tussenuitspraken), de kosten voor eventueel in te schakelen experts, de kosten voor afhandeling van de actie, waaronder de kosten voor de vaststelling, berekening, verdeling en administratie van uit te betalen schadevergoedingen, de kosten voor eventuele incasso- en executiemaatregelen en een eventuele (proces)kostenveroordeling ten nadele van Stichting ICAM. De Financier heeft deze toezegging gedaan op basis van gedetailleerde, zorgvuldige en adequate kostenramingen die Stichting ICAM heeft gemaakt. In de Financieringsovereenkomst is echter bepaald dat deze kostenramingen geen vaste posten betreffen maar inschattingen.

656. De Raad van Bestuur heeft onderzoek gedaan naar de kapitalisatie, het trackrecord en de reputatie van de externe Financier (Principe III.1). In dat kader hebben meerdere overleggen tussen Stichting ICAM en de Financier plaatsgevonden en is door de Financier relevante informatie verstrekt. Stichting ICAM heeft zich hierbij laten adviseren door haar advocaten, die in hun opdrachtovereenkomst hebben bevestigd dat zij, zolang zij werken voor Stichting ICAM, geen opdrachten van de Financier zullen aannemen en uitsluitend optreden ten behoeve van

Stichting ICAM en haar achterban (Principe III.4). Stichting ICAM heeft op basis van deze overleggen en informatie vast kunnen stellen dat de Financier ruim voldoende middelen ter beschikking heeft om deze collectieve actie te bekostigen.

657. Stichting ICAM beschikt aldus over voldoende middelen om deze collectieve vordering in te stellen.

658. Tegenover de financiering door de Financier, zijn Stichting ICAM en de Financier een redelijke vergoeding voor het financieringsrisico overeengekomen, zoals toegestaan conform Principe II.2 en Principe III van de Claimcode 2019 (randnummer 648).

659. In de Financieringsovereenkomst is een rechtskeuze voor Nederlands recht en een forumkeuze voor de rechtbank Amsterdam opgenomen. De Financier is een in Nederland gevestigde besloten vennootschap en de woonplaatskeuze in de Financieringsovereenkomst is dan ook Breda, Nederland (Principe III.2).

660. In de Financieringsovereenkomst is voorts vastgelegd dat Stichting ICAM volledig verantwoordelijk is en blijft voor de uitvoering van de collectieve actie en de volledige zeggenschap heeft over de actie en alle aspecten van haar activiteiten, waaronder de proces- en schikkingsstrategie en de inschakeling van dienstverleners en/of andere derden dan wel de beëindiging van de relatie daarmee (Principe III.3). Daarnaast is een regeling opgenomen over de vertrouwelijkheid van informatie en over de vraag tot welke informatie de Financier toegang heeft (Principe III.5). Verder is in de Financieringsovereenkomst afgesproken dat de Financier de overeenkomst niet kan opzeggen of ontbinden totdat een einduitspraak in eerste aanleg is verkregen, behoudens bijzondere omstandigheden (Principe III.6).

661. Op de Website is op de pagina “Veelgestelde vragen” vermeld dat sprake is van externe financiering en is vermeld wie de Financier is (**productie B.3**). Ook zijn de afspraken met de Financier op hoofdlijnen beschreven (Principe III.7). In het Verantwoordingsdocument op de Website wordt in de paragraaf “no cure, no pay” verdere uitleg gegeven over de externe financiering (**productie B.8**).

662. In de Financieringsovereenkomst is tot slot bedongen dat Stichting ICAM de nadere financieringsinformatie zoals beschreven in Principe III.8 aan de rechtbank mag meedelen indien de rechtbank dat verzoekt of beveelt. Indien en voor zover de rechtbank hiertoe aanleiding ziet, verzoekt Stichting ICAM om mededeling van die informatie voor te schrijven op zodanige wijze dat de Staat c.s. daarvan geen kennis kunnen nemen. Stichting ICAM is echter bereid, indien daartoe behoefte bestaat, in overleg te treden over het al dan niet geven van inzage aan de Staat c.s.in (delen van) de Financieringsovereenkomst.

Principe IV – Onafhankelijkheid en vermijding van belangentegenstelling

663. In artikel 6.2 en 13.2 van de Statuten (**productie B.1**) is opgenomen dat de leden van de Raad van Bestuur respectievelijk de Raad van Toezicht ten opzichte van elkaar, ten opzichte van de Raad van Toezicht respectievelijk de Raad van Bestuur en ten opzichte van de Financier onafhankelijk en kritisch moeten kunnen opereren. In artikel 18 van de Statuten is de uitwerking van Principe IV.1-3 volledig overgenomen. In dit artikel is vastgelegd dat binnen de Raad van Bestuur en de Raad van Toezicht alsmede tussen de leden van de Raad van Bestuur enerzijds en de Raad van Toezicht anderzijds, geen nauwe relaties mogen bestaan. Verder is vastgelegd dat eventuele belangen van de leden die aanleiding kunnen geven tot twijfel, op de Website worden gepubliceerd en dat Stichting ICAM geen overeenkomsten zal sluiten met organisaties waarbij een lid van de Raad van Bestuur of de Raad van Toezicht is betrokken. In artikel 21 van de Statuten is vastgelegd dat de leden van de Raad van Bestuur en de Raad van Toezicht en de advocaten van Stichting ICAM zelfstandig en onafhankelijk zijn van de Financier en dat de Financier onafhankelijk is van de Staat c.s.

664. Er wordt door Stichting ICAM, de leden van de Raad van Bestuur en de Raad van Toezicht, de Financier en de advocaten van Stichting ICAM volledig voldaan aan alle bovengenoemde vereisten uit de Claimcode 2019 en de Statuten.

Principe V – De samenstelling, taak en werkwijze van de Raad van Bestuur

665. De Raad van Bestuur bestaat uit drie leden en is evenwichtig samengesteld. Zoals in paragraaf 9.1.3.6 is beschreven zijn de leden van de Raad van Bestuur ervaren experts op juridisch en financieel gebied, zoals ook wordt voorgeschreven door artikel 6.2 en 6.3 van de Statuten.

666. In artikel 8 van de Statuten is vastgelegd dat Stichting ICAM wordt vertegenwoordigd door de Raad van Bestuur en dat die bevoegdheid tevens toekomt aan twee gezamenlijk handelende bestuurders. In artikel 7.3 van de Statuten is bepaald dat de Raad van Bestuur over het gevoerde beleid ten minste één keer per jaar verantwoording aflegt aan de Raad van Toezicht. In artikel 9.10 is bepaald dat ingrijpende besluiten goedkeuring van de Raad van Toezicht. De Raad van Toezicht kan overeenkomstig artikel 9.11 van de Statuten nader te bepalen besluiten aan haar goedkeuring onderwerpen. De balans en de staat van baten en lasten dienen ter goedkeuring te worden voorgelegd aan de Raad van Toezicht zoals bepaald in artikel 22.4 tot en met 22.7 van de Statuten. Verwezen wordt naar hetgeen is opgenomen in paragraaf 9.1.3.2, waarvan Stichting ICAM verzoekt het als hier herhaald en ingelast te beschouwen.

667. In overeenstemming met de Claimcode 2019 en artikel 12 van de Statuten houdt de Raad van Bestuur een algemeen toegankelijk website in stand: ten aanzien van Stichting ICAM in het algemeen betreft dat www.stichtingicam.nl en specifiek voor de collectieve actie de Website (www.datalek-ggd.nl). Op deze websites wordt de informatie zoals beschreven in Principe V.8 beschikbaar gesteld. Verwezen wordt naar hetgeen is opgenomen in paragraaf 9.1.3.5, waarvan Stichting ICAM verzoekt het als hier herhaald en ingelast te beschouwen.

Principe VI – Vergoedingen aan bestuurders

668. De uitwerking van Principe VI is overgenomen in artikel 10 van de Statuten. De leden van de Raad van Bestuur ontvangen voor de uitoefening van hun bestuurstaken een beloning die in redelijke verhouding staat tot de aard en intensiteit van hun werkzaamheden en een onkostenvergoeding. De leden ontvangen geen andere vergoeding voor hun werkzaamheden voor Stichting ICAM. De beloning en onkostenvergoeding is vastgesteld door de Raad van Toezicht. De hoofdlijnen van het beloningsbeleid zijn door Stichting ICAM opgenomen in het Verantwoordingsdocument dat beschikbaar is op de Website (**productie B.8**). De uiteindelijke vergoedingen van de leden van de Raad van Bestuur zullen worden gespecificeerd in de jaarrekening die op de Website zal worden gepubliceerd, voorzien van een toelichting.

Principe VII – De Raad van Toezicht

669. Stichting ICAM heeft een Raad van Toezicht die toezicht houdt op het beleid en de strategie van de Raad van Bestuur. De Raad van Toezicht bestaat uit drie leden waarvan er één kan worden benoemd op voordracht van de Financier. Deze voordracht wordt vermeld op de Website, bij het profiel van het betreffende lid (**productie B.3**). De leden van de Raad van Toezicht zijn ervaren en hebben expertise op juridisch en financieel gebied, zoals beschreven in paragraaf 9.1.3.2. De leden van de Raad van Toezicht kunnen onafhankelijk en kritisch opereren, zoals ook wordt voorgeschreven door artikel 13.2 van de Statuten.

670. Op dit moment bestaat de Raad van Toezicht uit twee leden vanwege het onverwachte overlijden van de heer [redacted]. Er wordt nog gezocht naar een vervangend lid met financiële expertise. De Financier is in de gelegenheid gesteld een kandidaat voor te dragen.

671. De Raad van Toezicht vergadert minimaal eenmaal per jaar, zoals wordt voorgeschreven door artikel 15.1 van de Statuten. De Raad van Toezicht en de Raad van Bestuur komen daarnaast minimaal eenmaal per jaar bijeen in een gemeenschappelijke vergadering zoals bepaald in artikel 17 van de Statuten. De Raad van Toezicht heeft voorts recht op informatie en inzage, en het verlenen van goedkeuring zoals onder meer bepaald in artikel 14.2 tot en met 14.4 en artikel 22.5 van de Statuten. De Raad van Toezicht zal verder, conform artikel 14.6 van de Statuten, jaarlijks een document opstellen waarin zij op hoofdlijnen verantwoording aflegt over het uitgevoerde toezicht, welk document op de Website wordt gepubliceerd (**productie B.1**).

672. De leden van de Raad van Toezicht ontvangen een door de gemeenschappelijke vergadering vastgestelde redelijke en niet bovenmatige onkostenvergoeding en vacatiegeld. De leden ontvangen daarnaast geen andere vergoeding voor hun werkzaamheden voor Stichting ICAM. De vergoedingen van de leden van de Raad van Toezicht zijn opgenomen in het Verantwoordingsdocument dat beschikbaar is op de Website (**productie B.8**) en zullen worden gespecificeerd in de jaarrekening die op de Website zal worden gepubliceerd, voorzien van een toelichting. Dit is vastgelegd in artikel 16 van de Statuten.

673. Verwezen wordt voorts naar hetgeen is opgenomen in paragraaf 9.1.3.2 waarvan Stichting ICAM verzoekt het als hier herhaald en ingelast te beschouwen.

9.1.4 Aanvullende ontvankelijkheidseisen

674. Artikel 3:305a lid 3 sub a tot en met c BW bevat een aantal aanvullende ontvankelijkheidseisen. Stichting ICAM voldoet ook aan deze vereisten.

9.1.4.1 Bestuurders hebben geen winstoogmerk

675. Op grond van artikel 3:305 lid 3 sub a BW mogen de leden van de Raad van Bestuur of hun opvolgers geen rechtstreeks of middellijk winstoogmerk hebben dat via de stichting wordt gerealiseerd. Bij de bespreking van Principe II van de Claimcode 2019 hiervoor heeft Stichting ICAM al toegelicht dat de leden van de Raad van Bestuur en van de Raad van Toezicht niet vrij kunnen beschikken over gelden van Stichting ICAM, anders dan ter uitvoering van hun taken in het belang van de stichting en haar achterban. Voorts hebben de leden van de Raad van Bestuur en de Raad van Toezicht geen relatie met of belang bij de verschillende dienstverleners die Stichting ICAM inschakelt voor de collectieve actie. De leden van de Raad van Bestuur en de Raad van Toezicht onderschrijven ieder het doel en de belangen van Stichting ICAM. Zij zetten hun ervaring en expertise in om dat doel te bereiken.

9.1.4.2 Voldoende nauwe band met de Nederlandse rechtssfeer

676. Op grond van artikel 3:305 lid 3 sub b BW moet de rechtsvordering een voldoende nauwe band hebben met de Nederlandse rechtssfeer. Daarvan is sprake als (i) het merendeel van de gedupeerden zijn gewone verblijfplaats in Nederland heeft, (ii) de gedaagden woonplaats in Nederland hebben en bijkomende omstandigheden wijzen op voldoende verbondenheid met de Nederlandse rechtssfeer of (iii) de gebeurtenis waarop de rechtsvordering betrekking heeft, heeft plaatsgevonden in Nederland. De collectieve vordering van Stichting ICAM voldoet aan dit vereiste.

677. Het merendeel van de Gedupeerden betreft Nederlandse ingezetenen die een test- of vaccinatieafspraak bij een GGD hebben gemaakt of zijn benaderd in verband met bron– en contactonderzoek. Voor een groot deel van de betreffende periode golden immers stringente reisbeperkingen en dus is niet aannemelijk dat een groot deel van de Gedupeerden personen betrof zonder gewone verblijfplaats in Nederland. Daarnaast zijn alle gedaagden gevestigd in Nederland en geldt als bijkomende omstandigheid waaruit de band met de Nederlandse rechtssfeer blijkt dat de gedaagden deel uitmaken van de Nederlandse overheid. Ten slotte heeft het GGD-datalek plaatsgevonden in Nederland, in systemen die werden/worden ingezet om de coronapandemie in Nederland te bestrijden.

9.1.4.3 Overleg met de Staat c.s.

678. Op grond van artikel 3:305a lid 3 sub c BW dient een belangenorganisatie in de gegeven omstandigheden voldoende te hebben getracht het gevorderde door het voeren van overleg met de verweerder te bereiken, waarbij een termijn van twee weken na de ontvangst door de verweerder van een verzoek tot overleg onder vermelding van het gevorderde, in elk geval voldoende is.

679. Stichting ICAM heeft ieder der Gedaagden per brief van 8 februari 2022 aangeschreven (**producties H.1A, H.2A, H.2B, H.2C, H.2N, H.3A, H.4A en H.5A**) en daarin uitgebreid en gemotiveerd uiteengezet op welke gronden zij de Gedaagden aanspreekt en waartoe de Gedaagden volgens haar verplicht zijn. Daarnaast hebben zij toegelicht welke schade de Gedupeerden hebben geleden en nog steeds lijden als gevolg van de schendingen door de Staat c.s. en wat de (totale) omvang van die schade is. Zij hebben de Staat c.s. voor die schade aansprakelijk gesteld. Stichting ICAM heeft ook verzocht verdere informatie te verstrekken en informatie over de Gedupeerden beschikbaar te houden zodat een toegewezen schadevergoeding kan worden uitgekeerd. In de brief heeft Stichting ICAM ieder der Gedaagden voorts uitgenodigd voor overleg over een oplossing buiten rechte. Zij hebben hen daarbij een termijn gegeven van drie weken om te bevestigen dat zij bereid waren tot overleg en een termijn van acht weken om dat overleg daadwerkelijk te laten plaatsvinden.

680. De Staat en GGD GHOR hebben ieder gereageerd dat zij tot overleg bereid waren. GGD GHOR heeft daarbij aangegeven dat zij het overleg mede namens de 25 GGD'en zou voeren. De correspondentie met (de advocaten van) de Staat en (de advocaten van) GGD GHOR wordt overgelegd in **productie H.1** respectievelijk **productie H.2**.

681. De Gemeenten zijn niet op de uitnodiging tot overleg ingegaan. Zij hebben (sommigen pas na een schriftelijke herinnering) aangegeven dat het ministerie het voortouw zou nemen in de contacten met Stichting ICAM (**productie H.3C**).

682. Ook de Veiligheidsregio's zijn niet op de uitnodiging tot overleg ingegaan. Het Veiligheidsberaad heeft namens alle 25 veiligheidsregio's dezelfde reactie gegeven als de Gemeenten (**productie H.5C**).

683. Op 6 april 2022 heeft Stichting ICAM met haar advocaten ten kantore van GGD GHOR overleg gevoerd met GGD GHOR en haar advocaten, die daarbij ook de 25 afzonderlijke GGD-en vertegenwoordigden. Naar aanleiding van dat overleg hebben (de advocaten van) GGD GHOR en (de advocaten van) Stichting ICAM schriftelijk verder gecorrespondeerd. Die correspondentie zag vooral op de verzoeken en sommaties om gegevens te bewaren van de Gedupeerden van het GGD-datalek, onder meer om, indien nodig, te kunnen bepalen welke van deze personen recht hebben op welk bedrag aan schadevergoeding en om met deze personen contact te kunnen opnemen. GGD GHOR heeft per brief van haar advocaten van 13 mei 2022 toegezegd dat zij die gegevens zal bewaren (**productie H.2J**). Daarnaast hebben Stichting ICAM en GGD GHOR

schriftelijke standpunten uitgewisseld over de doelstellingen van Stichting ICAM, waarbij GGD GHOR de ideële doelstellingen van Stichting ICAM in twijfel trok en suggereerde dat deze collectieve procedure primair zou dienen om commerciële belangen van de Financier te dienen, hetgeen vanzelfsprekend door Stichting ICAM is en wordt betwist.

684. GGD GHOR heeft uiteindelijk in een brief van 25 mei 2022 aangegeven dat het niet reëel lijkt te veronderstellen dat verder overleg tot een oplossing leidt (**productie H.2K**). Stichting ICAM heeft daarop per brief van 8 juli 2022 gereageerd, waarbij zij heeft aangegeven nog altijd bereid te zijn tot verder overleg (**productie H.2L**). GGD GHOR geeft in haar laatste brief van 21 juli 2022 aan dat zij in het licht van de hoogte van de schadevordering niet inziet hoe verder overleg tot een oplossing kan leiden (**productie H.2M**). Gezien deze opstelling heeft geen verder overleg plaatsgevonden.

685. Op 19 april 2022 heeft Stichting ICAM met haar advocaten ten kantore van het ministerie overleg gevoerd met het ministerie en haar advocaten. Naar aanleiding van dat overleg hebben (de advocaten van) de Staat en (de advocaten van) Stichting ICAM schriftelijk verder gecorrespondeerd. Het ministerie heeft aangegeven bereid te zijn met Stichting ICAM in overleg te treden over de wijze waarop de informatiebeveiliging bij de overheid kan verbeteren en welke rol Stichting ICAM daarbij kan vervullen, maar heeft alle aansprakelijkheid voor schade categorisch afgewezen. Stichting ICAM heeft per brief van 28 juli 2022 aangegeven in gesprek te willen gaan over het onderwerp van informatiebeveiliging en aangegeven dat zij ervan uitging dat de Staat niet bereid was tot overleg over de schade, maar dat Stichting ICAM ook ten aanzien van dat onderwerp graag beschikbaar bleef. Het ministerie heeft niet gereageerd op deze brief. Stichting ICAM gaat er dan ook van uit dat het ministerie niet bereid is tot verder overleg, maar blijft overigens zelf wel tot overleg bereid.

9.2 Artikel 80 AVG

9.2.1 Aan eventuele aanvullende ontvankelijkheidseisen is voldaan

686. Voor zover artikel 80 AVG aanvullende ontvankelijkheidseisen bevat, namelijk dat de belangenorganisatie geen winstoogmerk heeft, de statutaire doelstellingen het openbaar belang dienen en de belangenorganisatie actief is op het gebied van gegevensbescherming, voldoet Stichting ICAM ook daaraan. Uit de Statuten blijkt duidelijk dat Stichting ICAM een openbaar belang dient, namelijk het opkomen voor groepen gedupeerden en specifiek voor gedupeerden van schendingen van het recht op privacy en gegevensbescherming. In randnummer 646 e.v. is toegelicht dat Stichting ICAM geen winstoogmerk heeft. Aan het actief zijn op het gebied van gegevensbescherming als bedoeld in artikel 80 AVG hoeven vanuit een oogpunt van effectieve uitoefening van handhavingsmogelijkheden geen hoge eisen te worden gesteld.[299] Gelet op

[299] Rechtbank Amsterdam, 30 juni 2021, ECLI:NL:RBAMS:2021:3307 (*Data Privacy Stichting/Facebook c.s.*), r.o. 7.33.

hetgeen is aangevoerd in paragraaf 9.1.2, ontplooit Stichting ICAM daadwerkelijk activiteiten en is voldaan aan dit vereiste.

9.2.2 Artikel 80 lid 2 AVG staat niet in de weg aan een opt-out collectieve vordering tot schadevergoeding

687. In het vonnis in de zaak The Privacy Collective tegen Oracle en Saleforce van 29 december 2021 heeft de rechtbank Amsterdam het voor toekomstige WAMCA-zaken over privacyrechten van belang geacht om een geschilpunt over de verhouding tussen de WAMCA en de AVG te signaleren, hoewel het voor de uitkomst van die zaak niet relevant was (hierna het "**TPC-Vonnis**").[300] Partijen in die zaak hadden een verschillende uitleg van artikel 80 AVG. In de gesprekken met de Staat c.s. is dit geschilpunt door hen ook aangehaald. Stichting ICAM verwacht dat zij daar in onderhavige procedure ook op in zullen gaan. Zij vindt het daarom van belang om de verhouding tussen de WAMCA en AVG hierna te bespreken. Stichting ICAM zal concluderen dat artikel 80 AVG niet in de weg staat aan een opt-out collectieve vordering tot schadevergoeding op grond van een schending van de AVG.

688. In artikel 80 AVG is het volgende bepaald:

> "1. De betrokkene heeft het recht een orgaan, organisatie of vereniging zonder winstoogmerk dat of die op geldige wijze volgens het recht van een lidstaat is opgericht, waarvan de statutaire doelstellingen het openbare belang dienen en dat of 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, opdracht te geven de klacht namens hem in te dienen, namens hem de in artikelen 77, 78 en 79 bedoelde rechten uit te oefenen en namens hem het in artikel 82 bedoelde recht op schadevergoeding uit te oefenen, indien het lidstatelijke recht daarin voorziet.
>
> 2. De lidstaten kunnen bepalen dat een orgaan, organisatie of vereniging als bedoeld in lid 1 van dit artikel, over het recht beschikt om onafhankelijk van de opdracht van een betrokkene in die lidstaat klacht in te dienen bij de overeenkomstig artikel 77 bevoegde toezichthoudende autoriteit en de in de artikelen 78 en 79 bedoelde rechten uit te oefenen, indien het/zij van mening is dat de rechten van een betrokkene uit hoofde van deze verordening zijn geschonden ten gevolge van de verwerking."

689. Op grond van lid 1 van artikel 80 AVG kunnen betrokkenen belangenorganisaties opdracht geven om het recht op schadevergoeding ingevolge artikel 82 AVG uit te oefenen indien het lidstatelijk recht daarin voorziet.

690. Op grond van lid 2 van artikel 80 AVG kan een belangenorganisatie ook onafhankelijk van de opdracht van betrokkenen de in artikel 78 en 79 AVG bedoelde rechten uitoefenen, voor zover het nationale recht in die mogelijkheid voorziet. Dit tweede lid bevat in tegenstelling tot het

[300] Rb Amsterdam 29 december 2021, ECLI:NL:RBAMS:2021:7647 (*The Privacy Collective/Oracle en Salesforce*).

eerste lid geen verwijzing naar artikel 82 AVG, dat over schadevergoeding gaat. Overweging 142 AVG gaat daar wel op in:

> "(142) Wanneer een betrokkene van oordeel is dat inbreuk is gemaakt op zijn rechten uit hoofde van deze verordening, moet hij het recht hebben organen, organisaties of verenigingen zonder winstoogmerk, die overeenkomstig het recht van een lidstaat zijn opgericht, die statutaire doelstellingen hebben die in het publieke belang zijn en die actief zijn op het gebied van de bescherming van persoonsgegevens, te machtigen om namens hem een klacht in te dienen bij een toezichthoudende autoriteit, om namens betrokkenen het recht op een voorziening in rechte uit te oefenen, of om namens betrokkenen het recht op de ontvangst van een vergoeding uit te oefenen indien dit in het lidstatelijke recht is voorzien. De lidstaten kunnen bepalen dat deze organen, organisaties of verenigingen over het recht beschikken om, ongeacht een eventuele machtiging door een betrokkene, in die lidstaat een klacht in te dienen en over het recht op een doeltreffende voorziening in rechte, indien zij redenen hebben om aan te nemen dat de rechten van een betrokkene zijn geschonden als gevolg van een verwerking van persoonsgegevens die inbreuk maakt op deze verordening. Voor deze organen, organisaties of verenigingen kan worden bepaald dat zij niet het recht hebben om namens een betrokkene een vergoeding te eisen buiten de machtiging door de betrokkene om." (onderstreping door advocaat)

691. In Nederland vormen artikel 3:305a BW en titel 14A Rv de bedoelde lidstatelijke voorziening. Dit volgt ook uit artikel 37 UAVG, dat expliciet verwijst naar artikel 3:305a BW. In artikel 37 UAVG wordt verwezen naar artikel 3:305a BW en is bepaald dat een verwerking niet ten grondslag kan worden gelegd aan een collectieve vordering indien een betrokkene daartegen bezwaar heeft. Dit sluit aan op het opt-out systeem waarop de WAMCA is gebaseerd.

692. Uit het TPC-Vonnis blijkt dat door Oracle en Salesforce in die zaak is aangevoerd dat de mogelijkheid om onafhankelijk van de opdracht van de betrokkene bepaalde AVG-rechten uit te oefenen, niet het recht op schadevergoeding omvat, omdat in artikel 80 lid 2 AVG niet wordt verwezen naar artikel 82 AVG. Overweging 142 AVG zou volgens hen een vertaalfout bevatten omdat het woord "niet" op de verkeerde plaats zou staan. Ook is aangevoerd dat een collectieve actie op grond van de WAMCA wegens schending van de AVG in strijd is met Unierecht. De Uniewetgever zou een commerciële claimcultuur in de context van gegevensbescherming hebben willen voorkomen.

693. Geen van deze argumenten gaat echter op.

9.2.2.1 A contrario interpretatie van artikel 80 lid 2 AVG ligt niet voor de hand

694. Dat artikel 80 lid 2 AVG geen verwijzing bevat naar artikel 82 AVG betekent niet dat daarmee gegeven is dat collectieve schadevergoedingsvorderingen onafhankelijk van de opdracht van betrokkenen niet mogelijk zijn.

695. Ten eerste beoogt artikel 80 lid 2 AVG de lidstaten bevoegdheden te verlenen. De bepaling heeft niet tot doel restricties op te leggen. Het gegeven dat naar een bepaalde bevoegdheid niet wordt verwezen, betekent op zichzelf niet dat sprake is van een verbod.

696. Ten tweede is de bepaling optioneel geformuleerd ("De lidstaten kunnen bepalen […]"). De lidstaten hebben dus de discretionaire bevoegdheid deze bepaling al dan niet om te zetten in nationaal recht.

697. Ten derde blijkt ook uit de Nederlandse taalversie van overweging 142 dat lidstaten kunnen bepalen dat belangenorganisaties niet het recht hebben om onafhankelijk van de opdracht van de betrokkene namens hem schadevergoeding te vorderen. Lidstaten moeten dus actief regelen dat belangenorganisaties geen schadevergoeding namens betrokkenen kunnen vorderen zonder daartoe strekkende opdracht. In Nederland is de mogelijkheid om zonder opdracht schadevergoeding te vorderen op grond van de AVG niet uitgesloten. Integendeel, dit is met artikel 37 UAVG, artikel 3:305a BW en titel 14A Rv juist expliciet mogelijk gemaakt. Ook in onder meer Frankrijk en Spanje is het mogelijk om onafhankelijk van de opdracht van betrokkene een collectieve schadevergoedingsactie in te stellen.[301]

698. De bevoegdheid van de nationale wetgever om nadere invulling te geven aan de bepalingen van de AVG is in lijn met de systematiek van de verordening. De AVG bevat een groot aantal open clausules, zo ook artikel 80 lid 2 AVG.[302] Het HvJEU heeft dit bevestigd in het Meta-arrest:

> "57. In dit verband moet worden opgemerkt dat de AVG, zoals blijkt uit haar artikel 1, lid 1, gelezen in het licht van met name de overwegingen 9, 10 en 13 ervan, in beginsel de nationale regelgevingen inzake de bescherming van persoonsgegevens volledig beoogt te harmoniseren. De bepalingen van deze verordening bieden de lidstaten evenwel de mogelijkheid om strengere of afwijkende nationale bepalingen vast te stellen die hun een beoordelingsmarge laten met betrekking tot de wijze waarop deze regels kunnen worden toegepast („open clausules").
> 58. Er zij immers aan herinnerd dat volgens vaste rechtspraak van het Hof bepalingen van verordeningen krachtens artikel 288 VWEU en wegens hun aard en hun functie in het systeem van de bronnen van het Unierecht in het algemeen rechtstreekse werking hebben in de nationale rechtsorden, zonder dat de nationale autoriteiten uitvoeringsmaatregelen hoeven vast te stellen. Voor sommige bepalingen kan het evenwel noodzakelijk zijn dat door de lidstaten nationale maatregelen ter uitvoering ervan worden vastgesteld (arrest van 15 juni 2021, Facebook Ireland e.a., C-645/19, EU:C:2021:483, punt 110 en aldaar aangehaalde rechtspraak).
> 59. Dit geldt met name voor artikel 80, lid 2, AVG, dat de lidstaten een beoordelingsmarge laat bij de uitvoering ervan. Om de gelegenheid te bieden zonder opdracht een representatieve vordering ter bescherming van persoonsgegevens in te stellen zoals bedoeld in deze bepaling, moeten de

[301] A. Pato, 'The National Adaptation of Article 80 GDPR, Towards the Effective Private Enforcement of Collective Data Protection Right', *National Adaptations of the GDPR (E-Conference*), 2019, p. 103-104.
[302] M.C. Samsom, annotatie bij Rb Amsterdam 29 december 2021, ECLI:NL:RBAMS:2021:7647 (*The Privacy Collective/Oracle en Salesforce*).

> lidstaten dus gebruikmaken van de door deze bepaling geboden mogelijkheid om deze vorm van vertegenwoordiging van betrokkenen op te nemen in hun nationale recht."[303]

699. Ten vierde verzetten de doelstellingen van de AVG en de goede werking van EU-recht zich tegen een a contrario interpretatie. De AVG beoogt betrokkenen een zo hoog mogelijk niveau van gegevensbescherming te bieden. Gelet op de beoogde volle en effectieve werking van de AVG is het vanzelfsprekend dat collectief schadeverhaal wegens schendingen van de AVG mogelijk is. Artikel 80 AVG heeft juist als doel om de privaatrechtelijke handhaving van het gegevensbeschermingsrecht te versterken, mede gegeven dat dit voor Betrokkenen vaak de enige mogelijkheid is om hun rechten te verwezenlijken (zie ook paragraaf 9.1.1). In dat kader is het niet voorstelbaar dat de Uniewetgever collectief schadeverhaal onafhankelijk van de opdracht van betrokkenen heeft willen uitsluiten.[304]

700. Ten vijfde is het onwaarschijnlijk dat de Uniewetgever in de procedurele autonomie van lidstaten heeft willen treden door collectief schadeverhaal op grond van artikel 80 lid 2 AVG uit te sluiten. In beginsel is het aan de lidstaten om procedures zo in te richten dat de effectieve werking van het Unierecht gewaarborgd wordt. Het Unierecht biedt daarentegen wel waarborgen tegen het geval waarin nationale procedurele regels de effectiviteit van het Unierecht beperken. Een nationale regeling zoals de WAMCA versterkt echter juist de effectiviteit van de AVG. De beperking zoals aangevoerd door de gedaagden in de TPC-zaak zou dan een opvallende en onwaarschijnlijke afwijking vormen van het beginsel van procedurele autonomie.[305] Artikel 80 lid 2 AVG laat lidstaten juist zelf de ruimte om in nationale wetgeving nadere (procedurele) invulling te geven aan het bepaalde in dat artikel, conform de hierboven aangeduide systematiek van open clausules. Daarmee geeft de Uniewetgever er blijk van dat zij op het punt van vertegenwoordiging van betrokkenen geen geharmoniseerde uniforme aanpak heeft beoogd.

701. Ten zesde is relevant dat artikel 80 lid 2 AVG wel expliciet verwijst naar artikel 79 AVG. In dat artikel wordt bepaald dat betrokkenen het recht hebben om een doeltreffende voorziening in rechte in te stellen tegen een verwerkingsverantwoordelijke die beweerdelijk inbreuk maakt op de AVG. Een dergelijke doeltreffende voorziening omvat bij uitstek een vordering tot schadevergoeding.

702. Voorgaande is door de Nederlandse regering bevestigd in de memorie van toelichting bij het wetsvoorstel ter implementatie van de Richtlijn Representatieve Vorderingen:

> "Onder een doeltreffende voorziening valt ook het recht op het vragen van schadevergoeding. Dit blijkt onder meer uit de laatste zin van overweging 142 AVG. Daarin staat dat "kan worden bepaald dat zij [(de organisaties)] niet het recht hebben om namens een betrokkene een vergoeding te eisen

[303] Hof van Justitie 28 april 2022, ECLI:EU:C:2022:322 (*Meta Platforms Ireland*), r.o. 57-59.
[304] M.C. Samsom, annotatie bij Rb Amsterdam 29 december 2021, ECLI:NL:RBAMS:2021:7647 (*The Privacy Collective/Oracle en Salesforce*).
[305] D.L. Barbiers & T.F. Walree, annotatie bij: Rb Amsterdam 29 december 2021, ECLI:NL:RBAMS:2021:7647 (The Privacy Collective/Oracle en Salesforce).

> buiten de machtiging door de betrokkene om [cursivering aangebracht].” Met andere woorden: het recht om schadevergoeding te vorderen in een collectieve actie, zonder voorafgaande volmacht van een belanghebbende, behoort in beginsel tot hetgeen de lidstaten kunnen regelen. Lidstaten mogen het recht op schadevergoeding wegens schending van de AVG in een collectieve actie, zonder volmacht van de betrokkene, dus regelen, maar zij hoeven dit niet.”[306]

703. In Nederland is dit zoals gezegd geregeld in artikel 37 UAVG, waarin het volgende is bepaald:

> “Een verwerking kan niet ten grondslag worden gelegd aan een vordering als bedoeld in artikel 305a, van Boek 3 van het Burgerlijk Wetboek of een beroep ingesteld in een bestuursrechtelijke procedure door een belanghebbende in de zin van artikel 1:2, derde lid, van de Algemene wet bestuursrecht, voor zover degene die door deze verwerking wordt getroffen, daartegen bezwaar heeft.”

704. Voorgaande wordt bevestigd in de memorie van antwoord bij het wetsvoorstel ter implementatie van de Richtlijn Representatieve Vorderingen:

> “De leden van de VVD-fractie geven ook terecht aan dat artikel 80 lid 2 AVG niet verwijst naar artikel 82 AVG (het recht op schadevergoeding), terwijl artikel 80 lid 1 AVG dat wel doet. Toch zijn er redenen om aan te nemen dat een collectieve schadevergoedingsactie is toegestaan volgens artikel 80 lid 2 AVG. Zo sluiten dit artikel en de AVG in het algemeen een vordering tot schadevergoeding zonder instemming van betrokkenen in een collectieve actie niet expliciet uit. Artikel 80 lid 2 AVG maakt collectieve acties zonder instemming van de betrokkenen wel expliciet mogelijk voor het instellen van een doeltreffende voorziening (artikel 79 AVG). De AVG bepaalt daarbij niet dat een vordering tot schadevergoeding geen doeltreffende voorziening is. Het feit dat de vordering tot schadevergoeding apart is geregeld in artikel 82 AVG doet hier niet aan af. In het algemeen is de volle en effectieve werking van de AVG nog een argument om aan te nemen dat artikel 80 lid 2 AVG ook het recht op schadevergoeding omvat. De volle en effectieve werking brengt mee dat betrokkenen hun privacy-rechten onder de AVG voldoende kunnen handhaven. De AVG voorziet ook in een recht op schadevergoeding voor betrokkenen bij een inbreuk op persoonsgegevens. De volle en effectieve werking houdt daarom ook in dat betrokkenen voldoende effectieve mogelijkheden moeten hebben om die schade vergoed te kunnen krijgen. De mogelijkheid van een collectieve actie is daarvoor een van de geschikte middelen.”[307]

9.2.2.2 Overweging 142 bevat geen vertaalfout

705. Verder is blijkens het TPC-Vonnis door Oracle en Salesforce gesteld dat overweging 142 AVG een “hinderlijke vertaalfout” zou bevatten. De Nederlandse taalversie van de laatste zin van overweging 142 AVG luidt:

---

306 *Kamerstukken II* 2021/22, 36 034, nr. 3, p. 9.
307 *Kamerstukken I*, 2022-2023, 36034, nr. B, p. 3 (**productie D.12**).

> "[…] Voor deze organen, organisaties of verenigingen kan worden bepaald dat zij niet het recht hebben om namens een betrokkene een vergoeding te eisen buiten de machtiging door de betrokkene om." (onderstreping door advocaat)

706. Volgens Oracle en Salesforce had de zin moeten luiden:

> "Voor deze organen, organisaties of verenigingen kan niet worden bepaald dat zij […] het recht hebben om namens een betrokkene een vergoeding te eisen buiten de machtiging door de betrokkene om."[308] (onderstreping door advocaat)

707. Zij baseren dat standpunt waarschijnlijk met name op de Engelse taalversie:

> "That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate."

708. De Nederlandse tekst spreekt duidelijk in het voordeel van het standpunt van Stichting ICAM. Datzelfde geldt voor de Italiaanse vertaling.[309] De Franse en Duitse taalversies van overweging 142 lijken echter weer tegen dat standpunt te spreken. In deze versies is neergelegd dat niet bepaald kan worden dat collectieve belangenorganisaties een schadevergoedingsvordering kunnen instellen onafhankelijk van de opdracht van een betrokkene, dit terwijl in Frankrijk het juist wel het mogelijk is om onafhankelijk van de opdracht van betrokkene een collectieve schadevergoedingsactie in te stellen.[310]

709. Stichting ICAM stelt voorop dat elke taalversie van de AVG – ook de Nederlandse - authentiek is. Het is dus niet zo dat bijvoorbeeld de Engelse taalversie leidend is en dat de andere taalversies daarvan zijn afgeleid. Van vertaalfouten kan formeel gezien dus helemaal geen sprake zijn. Bovendien ligt het ook niet voor de hand dat feitelijk gezien sprake is geweest van een vertaalfout.

710. Ten eerste is de Engelse taalversie ambigu, nu niet duidelijk is welke betekenis aan "may not" moet worden toegekend. De betekenis daarvan kan evengoed zijn dat "het mogelijk is" dat lidstatelijk recht uitsluit om onafhankelijk van de opdracht van betrokkene een collectieve schadevergoedingsactie in te stellen.

711. Ten tweede is de tekst van artikel 80 en van overweging 142 AVG blijkens de totstandkomingsgeschiedenis van de AVG het resultaat van een compromis. Uit die totstandkomingsgeschiedenis blijkt dat de Raad er op tegen leek te zijn om in artikel 80 AVG (artikel 76 ten tijde van de ontwerptekst) op te nemen dat een collectieve

---

[308] Rb Amsterdam 29 december 2021, ECLI:NL:RBAMS:2021:7647 (*The Privacy Collective/Oracle en Salesforce*), r.o. 5.22.

[309] D.L. Barbiers & T.F. Walree, annotatie bij: Rb Amsterdam 29 december 2021, ECLI:NL:RBAMS:2021:7647 (*The Privacy Collective/Oracle en Salesforce*).

[310] A. Pato, 'The National Adaptation of Article 80 GDPR, Towards the Effective Private Enforcement of Collective Data Protection Right', *National Adaptations of the GDPR (E-Conference*), 2019, p. 103-104.

schadevergoedingsvordering ook zonder opdracht daartoe van betrokkenen ingesteld mocht worden. In een nota van 1 juni 2015 wordt namelijk het volgende tekstvoorstel gedaan:

> "112) … Member States may provide that such a body, organisation or association should have the right to lodge, independently of a data subject's mandate, a complaint and/or have the right to an effective judicial remedy where it has reasons to consider that a personal data breach referred to in Article 32(1) has occurred and Article 32(3) does not apply the rights of a data subject's right have been infringed as a result of the processing of personal data which are not in compliance with this Regulation. This body, organisation or association does not have the right to claim compensation on a data subject's behalf."[311] (onderstreping door advocaat)

712. De voetnoot bij deze passage vermeldt dat de uitsluiting van deze mogelijkheid een verzoek was van Nederland.

713. Het Europees Parlement was daarentegen wél voor het opnemen van deze mogelijkheid:

> "In Article 76(1) and (2), the European Parliament insists on adding a reference to Article 77. Since such an addition is not acceptable for Council, the European Parliament proposes to introduce such reference only in Article 76(1) and to further frame the notion of the bodies, organizations or associations that would be able to act, possibly by referring to the non-profit making character of the organisations and/or their public interest objectives as an addition to the protection of personal data. The Presidency considers that these elements could be an avenue for finding a compromise."[312]

714. Bedoeld is dan ook om lidstaten in staat te stellen zelf invulling te geven aan artikel 80 lid 2 AVG, om zo het tussen de Raad en het Parlement bereikte compromis gestalte te geven, hetgeen in de uiteindelijke Engelse taalversie heeft geleid tot de woorden "may not" ter vervanging van de woorden "does not".

715. In de memorie van antwoord bij het wetsvoorstel ter implementatie van de Richtlijn Representatieve Vorderingen geeft de Nederlandse regering nadere context aan de bedoelingen ten tijde van de totstandkoming van overweging 142 AVG, hetgeen het voorgaande bevestigd. In antwoord op een vraag die onder meer ziet op de verenigbaarheid van de AVG met de WAMCA, licht de regering als volgt toe:

> "Ten tijde van de onderhandelingen over de mogelijkheden voor collectieve actie in de AVG was de Wet afwikkeling massaschade in collectieve actie (WAMCA) in voorbereiding, maar dus nog geen wet. Onder het oude artikel 3:305a van het Burgerlijk Wetboek (BW) kon een collectieve actie niet strekken tot het verkrijgen van schadevergoeding in geld. Er bestonden in Nederland daarom op dat moment ook geen regels voor collectieve schadevergoedingsacties, want dat soort acties was er niet. De voorstellen voor de WAMCA waren erop gericht om een collectieve schadevergoedingsactie in Nederland mogelijk te maken met voldoende waarborgen voor de toegang en voor de procedure.

311 Raad van de Europese Unie 1 juni 2015, Nota 2012/0011(COD) 9398/15, p. 66.
312 Raad van de Europese Unie 30 oktober 2015, Nota 2012/0011(COD) 13606/15, p. 3.

> Daartoe werden de eisen voor het mogen instellen van een collectieve actie aangescherpt (met een uitzonderingsmogelijkheid voor ideële acties). Ook bevatte het WAMCA-voorstel een geheel eigen procedure voor collectieve acties in een nieuwe titel 14A van het Wetboek van Burgerlijke Rechtsvordering (Rv). De procedure in het WAMCA-voorstel ging uit van een opt out, dus een collectieve actie zonder machtiging van een benadeelde, ook als de actie strekte tot verkrijging van schadevergoeding.
> De regeling voor collectieve acties in artikel 3:305a BW is altijd een horizontale regeling geweest. Dat wil zeggen dat die regeling altijd ook al van toepassing op collectieve acties wegens onrechtmatige gegevensverwerking. Voor Nederland was daarom vooral belangrijk dat de AVG de Nederlandse horizontale regeling zo min mogelijk zou doorkruisen. De AVG doet dat deels wel, door een eigen criterium in artikel 80 lid 1 van die verordening voor de organisaties die onder de AVG een collectieve actie kunnen instellen. De Nederlandse inzet was om te voorkomen dat de AVG daarnaast rechtstreeks mogelijk zou maken dat een organisatie zonder machtiging van een betrokkene (collectief) schadevergoeding kon vorderen. Dan zou Nederland zelf immers geen nadere voorwaarden kunnen stellen aan een collectieve schadevergoedingsactie wegens onrechtmatige gegevensverwerking. Nederland wilde daarom dat de lidstaten zelf konden bepalen of en hoe zij mogelijk maakten dat een organisatie op basis van de AVG een collectieve schadevergoedingsactie kon instellen. Zo zou Nederland, afhankelijk van de uitkomsten van het wetgevingsproces van de WAMCA, collectieve schadevergoedingsacties zonder machtiging van de betrokkene al dan niet kunnen toelaten.
> De op verzoek van Nederland aangepaste bewoordingen van overweging 142 AVG sluiten in de Nederlandse taalversie geheel aan bij die Nederlandse inzet. De bewoordingen laten de lidstaten de ruimte om een opt out schadevergoedingsactie toe te staan, maar ook om dit niet te doen. Met de komst van de WAMCA per 1 januari 2020 kan een organisatie die voldoet aan de eisen van artikel 80 AVG in Nederland daarom een collectieve schadevergoedingsactie wegens schending van de AVG instellen op basis van titel 14A Rv."[313] (onderstreping door advocaat)

9.2.2.3 Uniewetgever wilde "commerciële claimcultuur" voorkomen, niet legitieme collectieve schadevorderingen

716. Uit het TPC-Vonnis blijkt verder dat door Oracle en Salesforce is aangevoerd dat de Uniewetgever een commerciële claimcultuur in de context van gegevensbescherming zou hebben willen voorkomen. Dat is in zoverre juist dat dit aan de orde is geweest tijdens de totstandkoming van de AVG.[314] Belangrijk is echter dat de Uniewetgever het specifiek heeft over een "commerciële claimcultuur". De nadruk ligt op het woord "commerciële" en op het voorkomen van uitwassen met belangenorganisaties die uitsluitend optreden vanwege eigen commerciële belangen of die van financiers. Wat de Uniewetgever heeft bedoeld is dat moet worden gewaarborgd dat belangenorganisaties collectieve acties met de juiste intenties voeren, zonder eigen commerciële belangen en zonder excessieve verdienmodellen van de diverse bij een massaschade-procedure

[313] *Kamerstukken I*, 2022-2023, 36034, nr. B, p. 2 en 3 (**productie C.18**).
[314] Zie onder meer de ontwerpmotivering van de Raad van de Europese Unie bij de AVG: Nota 2012/0011(COD) 5419/16, te raadplegen via: https://data.consilium.europa.eu/doc/document/ST-5419-2016-ADD-1-REV-1/nl/pdf.

betrokken partijen. Dit kan worden gewaarborgd door eisen te stellen aan (de governance van) deze belangenorganisaties. Voorgaande blijkt uit de Ontwerpmotivering van de Raad:

> "9.2. Representation of data subjects - A data subject has the right to mandate bodies, organisations or associations that fulfil specific criteria, such as working on a non-profit basis and being active in the field of data protection, to lodge the complaint on his or her behalf and to exercise the rights of judicial remedy on his or her behalf and to exercise the right to receive compensation on his or her behalf if provided for by Member State law. These specific criteria aim to avoid the development of a commercial claims culture in the field of data protection."[315] (onderstreping door advocaat)

717. Van een dergelijke commerciële claimcultuur zal in Nederland geen sprake zijn, omdat artikel 3:305a BW strenge eisen stelt aan de inrichting van belangenorganisaties. Bij de totstandkoming van de WAMCA is ook aandacht besteed aan de mogelijkheid van een claimcultuur en zijn juist eisen geformuleerd om dit te voorkomen. In de memorie van toelichting bij de WAMCA wordt in dit kader gewezen op artikel 3:305a lid 2 onderdeel c BW waarin de eis is gesteld dat belangenorganisaties over voldoende financiële middelen moeten beschikken om de procedure te voeren. Belangenorganisaties kunnen in de procedure worden gevraagd om dit te onderbouwen. Toetsing aan dit vereiste in combinatie met de andere vereisten die aan de belangenorganisaties worden gesteld zoals het waarborgvereiste, geeft de rechter de mogelijkheid om te kijken naar financieringsconstructies. Het biedt de rechter een handvat voor het uitsluiten van gevallen waarin externe financiering de belangen van de gedupeerden negatief beïnvloedt.[316]

718. Ook zijn de principes uit Claimcode 2019 er mede op gericht een commerciële claimcultuur te voorkomen. In de Claimcode wordt daarover het volgende opgemerkt:

> "Hoewel procesfinanciering nog wel eens geassocieerd wordt met 'claimcultuur' of 'Amerikaanse toestanden', is men in de literatuur minder bevreesd. Van Boom schrijft bijvoorbeeld dat externe financiering niet tot een toename in 'unmeritorious' claims leidt, maar juist tot een filterwerking, omdat financiers hun zaken grondig selecteren. Daarnaast stellen verschillende auteurs dat externe financiering de toegang tot het recht vergroot en bijdraagt aan een gelijk speelveld."[317]

719. Het standpunt dat nu de Uniewetgever een commerciële claimcultuur heeft willen voorkomen, het niet mogelijk zou zijn om een collectieve schadevergoedingsactie te voeren wegens schending van de AVG is dus niet juist.

720. Bij monde van de minister voor Rechtsbescherming concludeert de Nederlandse regering in de memorie van antwoord bij het wetsvoorstel ter implementatie van de Richtlijn Representatieve Vorderingen dan ook uiteindelijk als volgt:

---

315 Raad van de Europese Unie 31 maart 2016, Nota 2012/0011(COD) 5419/16, p. 30-31.
316 *Kamerstukken II* 2016/17, 34608, nr. 3 (MvT), zie ook de Claimcode p. 18-19 (**productie B.2**).
317 Claimcode, p. 33 (**productie B.2**).

> "Al met al zijn er m.i. voldoende aanknopingspunten om aan te nemen dat de AVG niet in de weg staat aan een collectieve actieregeling onder de WAMCA, dus zonder instemming van de betrokkenen."[318]

9.2.3 Subsidiair: nalaten om gebruik te maken van opt-out geldt als opdracht van betrokkenen

721. Mocht de rechtbank toch tot de conclusie komen dat Stichting ICAM een opdracht van Betrokkenen nodig heeft voor deze collectieve schadevordering, dan voert Stichting ICAM subsidiair aan dat het nalaten om gebruik te maken van de opt-out mogelijkheid die de WAMCA biedt heeft te gelden als een zodanige opdracht.[319] Artikel 1018f lid 1 Rv gaat immers uit van een impliciete machtiging van de personen uit de nauw omschreven groep. Zij stemmen in met de procedure tot het moment dat expliciet gebruik wordt gemaakt zich te bevrijden van deelname.

9.3 Collectieve schadevergoedingsvordering onafhankelijk van opdracht op grond van artikel 7 en 8 Handvest, artikel 8 EVRM en onrechtmatige daad

722. Ongeacht het oordeel van de rechtbank over de vraag of artikel 80 lid 2 AVG in de weg staat aan een collectieve vordering tot schadevergoeding op grond van de WAMCA, en over de vraag of het nalaten om gebruik te maken van de opt-out mogelijkheid geldt als opdracht van de betrokkene, geldt hoe dan ook dat artikel 7 en 8 Handvest, artikel 8 EVRM, (paragraaf 4.1), artikel 6:162 BW (paragraaf 6.2) en 6:170 BW (paragraaf 6.3) onafhankelijk van de opdracht van Gedupeerden ten grondslag kunnen worden gelegd aan de in deze procedure ingestelde vordering tot schadevergoeding.

723. De AVG laat blijkens overweging 146 schadevergoedingsacties op grond van inbreuken op andere regels van het nationale- of Unierecht immers onverlet:

> "De verwerkingsverantwoordelijke of de verwerker moeten alle schade vergoeden die iemand kan lijden ten gevolge van een verwerking die inbreuk maakt op deze verordening. De verwerkingsverantwoordelijke of de verwerker moet van zijn aansprakelijkheid worden vrijgesteld indien hij bewijst dat hij niet verantwoordelijk is voor de schade. Het begrip "schade" moet ruim worden uitgelegd in het licht van de rechtspraak van het Hof van Justitie, op een wijze die ten volle recht doet aan de doelstellingen van deze verordening. Dit laat eventuele eisen tot schadeloosstelling wegens inbreuken op andere regels in het Unierecht of het lidstatelijke recht onverlet. […]" (onderstreping door advocaat)

724. Artikel artikel 7 en 8 Handvest, artikel 8 EVRM, artikel 6:162 BW, artikel 6:170 BW en de specifieke zorgwetgeving kunnen dan ook als zelfstandige grondslag dienen voor een collectieve

[318] *Kamerstukken I*, 2022-2023, 36034, nr. B, p. 3 (**productie C.18**).
[319] Zie ook: M.C. Samsom, annotatie bij Rb Amsterdam 29 december 2021, ECLI:NL:RBAMS:2021:7647 (*The Privacy Collective/Oracle en Salesforce*).

vordering tot schadevergoeding op basis van de WAMCA en haar opt-out systeem. Een expliciete opdracht van Betrokkenen is daarvoor niet nodig.[320]

9.4 Vereisten ex artikel 1018c lid 1 en lid 5 Rv

725. Artikel 1018c lid 1 Rv vereist dat een dagvaarding waarmee een collectieve actie bedoeld in artikel 3:305a BW wordt ingesteld, de volgende informatie vermeldt:

a) Een omschrijving van de gebeurtenis of de gebeurtenissen waarop de collectieve vordering betrekking heeft. Deze informatie is opgenomen in de eerdere hoofdstukken van deze Dagvaarding;

b) Een omschrijving van de personen tot bescherming van wier belangen de collectieve vordering strekt. Deze informatie is opgenomen in paragraaf 9.1.1;

c) Een omschrijving van de mate waarin de te beantwoorden feitelijke en rechtsvragen gemeenschappelijk zijn. Deze informatie is opgenomen in paragraaf 9.1.1 en 9.4.1;

d) Een omschrijving van de wijze waarop voldaan is aan de ontvankelijkheidseisen van artikel 3:305a lid 1 t/m 3 BW of van de gronden waarop het zesde lid van dat artikel van toepassing is. Deze informatie is opgenomen in paragraaf 9.1;

e) Gegevens die de rechter in staat stellen om voor deze collectieve vordering een Exclusieve Belangenbehartiger aan te wijzen, voor het geval andere collectieve vorderingen voor dezelfde gebeurtenis overeenkomstig artikel 1018d worden ingesteld. Deze informatie is opgenomen in paragraaf 9.4.2;

f) De verplichting van de eiser om van de zaak aantekening te maken in het register, bedoeld in artikel 1018c lid 2 Rv, en om te vermelden wat ingevolge dit artikel de gevolgen zijn van die aantekening. Deze informatie is opgenomen in paragraaf 9.4.3 hieronder.

726. Artikel 1018c lid 5 Rv bepaalt voorts dat inhoudelijke behandeling van een collectieve vordering slechts plaatsvindt indien en nadat de rechter heeft beslist:

a) Dat eiser voldoet aan de ontvankelijkheidseisen van artikel 3:305a BW. Dit wordt onderbouwd in paragraaf 9.1;

b) Dat eiser voldoende aannemelijk heeft gemaakt dat het voeren van de collectieve vordering efficiënter en effectiever is dan het instellen van een individuele vordering doordat de te beantwoorden feitelijke en rechtsvragen in voldoende mate

[320] Zie ook: D.L. Barbiers & T.F. Walree, annotatie bij: Rb Amsterdam 29 december 2021, ECLI:NL:RBAMS:2021:7647 (*The Privacy Collective/Oracle en Salesforce*).

gemeenschappelijk zijn, het aantal personen tot bescherming van wier belangen de vordering strekt, voldoende is en, indien de vordering strekt tot schadevergoeding, dat zij alleen dan wel gezamenlijk een voldoende groot financieel belang hebben. Dit wordt toegelicht in paragraaf 9.1.1; en

c) Dat niet summierlijk van de ondeugdelijkheid van de collectieve vordering blijkt op het moment waarop het geding aanhangig wordt. Dit wordt toegelicht in paragraaf 9.4.4 hieronder.

9.4.1 Feitelijke en rechtsvragen zijn voldoende gemeenschappelijk

727. Het voeren van deze collectieve actie is efficiënter en effectiever dan het instellen van individuele vorderingen.

728. De te beantwoorden feitelijke en rechtsvragen zijn in voldoende mate gemeenschappelijk voor alle personen binnen de Groep Gedupeerden. Zowel de normschending als de feiten, de causaliteit en de schade zijn (voldoende) abstraheerbaar van de belangen van individuele Gedupeerden. Stichting ICAM verzoekt hetgeen is opgenomen in paragraaf 9.1.1 als hier herhaald en ingelast te beschouwen.

729. Collectieve behandeling van de schade van de Gedupeerden is daarnaast wenselijk. Het aantal Gedupeerden is ongekend groot, minstens 6,5 miljoen mensen. De schade per Gedupeerde bedraagt € 500,- aan immateriële schade in Gedupeerden Categorie A en € 1.500,- aan immateriële in Gedupeerden Categorie B. Samen met de materiële schade per persoon van € 50,- komt het totale schadebedrag komt daarmee op ongeveer € 3.576.250.000,-, exclusief wettelijke rente. De ingestelde vordering is derhalve zeer groot en dus ruimschoots voldoende om afwikkeling in het kader van de WAMCA te rechtvaardigen.

9.4.2 Stichting ICAM als Exclusieve Belangenbehartiger

730. Op het moment van het uitbrengen van deze Dagvaarding is Stichting ICAM niet bekend met andere belangenorganisaties die opkomen voor de belangen van de Gedupeerden. Het is echter mogelijk dat andere partijen gedurende de periode van drie maanden dat deze collectieve actie in het register is ingeschreven alsnog een dagvaarding indienen. Voor het geval dat ook andere belangenorganisaties vanwege het GGD-datalek een collectieve vordering zullen instellen op grond van artikel 1018d Rv, vordert Stichting ICAM om haar op grond van artikel 1018e lid 1 Rv als Exclusieve Belangenbehartiger te benoemen.

731. Stichting ICAM stelt zich voor dat geval reeds nu op het standpunt dat zij het meest geschikt is om als Exclusieve Belangenbehartiger op te treden voor de Gedupeerden. Op grond van artikel 1018e lid 1 Rv is daartoe allereerst van belang dat Stichting ICAM voldoet aan de ontvankelijkheidseisen van artikel 3:305a lid 1 t/m 3 BW. Dat Stichting ICAM aan deze eisen

voldoet is hiervoor toegelicht (paragraaf 9.1). Verder dienen op grond van artikel 1018e lid 1 sub a t/m d de volgende omstandigheden in aanmerking te worden genomen, op grond waarvan Stichting ICAM meent dat zij geschikt is om als Exclusieve Belangenbehartiger te worden aangewezen:

a) **De omvang van de groep personen voor wie de eiser opkomt**. Stichting ICAM komt op voor ten minste 6,5 miljoen Gedupeerden en heeft een zeer omvangrijke aanhang van 133.691 Deelnemers. Dat is een ongekend hoog aantal actief aangeslotenen voor een collectieve actie. Naar verwachting zal dat aantal verder groeien (paragraaf 9.1.3.1);

a) **De grootte van het door deze groep vertegenwoordigde financiële belang**. Het uiteindelijke financiële belang van de door Stichting ICAM vertegenwoordigde groep Gedupeerden zal worden bepaald door de hoogte van de schadevergoeding die door de rechtbank wordt toegekend per (categorie) Gedupeerde(n). Op basis van de huidige stand van de rechtspraak meent Stichting ICAM echter dat het totale financiële belang dient te worden begroot op een bedrag van € 3.576.250.000,- (paragraaf 1.3);

b) **Andere werkzaamheden die de eiser verricht voor de personen voor wie zij opkomt in of buiten rechte**. Volgens de wetgever kunnen die andere werkzaamheden bijvoorbeeld zien op het optreden als spreekbuis voor benadeelden of andere activiteiten op basis waarvan juist deze belangenbehartiger in beeld komt om voor de hele groep personen op te treden:[321] Stichting ICAM verwijst voor de werkzaamheden die zij verricht naar paragraaf 9.1.2;

c) **Eerder door de eiser verrichte werkzaamheden of ingestelde collectieve vorderingen**. Die eerdere werkzaamheden kunnen wijzen op de benodigde deskundigheid en ervaring voor het voeren van een collectieve vordering en het optreden daarin als Exclusieve Belangenbehartiger:[322] Stichting ICAM verwijst hiervoor naar paragraaf 9.1.3.6.

9.4.3 Aantekening in het centraal register collectieve voor collectieve vorderingen en de gevolgen daarvan

732. Stichting ICAM zal het exploot van de Dagvaarding tijdig, binnen twee dagen na de dag van dagvaarding, ter griffie indienen onder gelijktijdige aantekening van de Dagvaarding in het centraal register voor collectieve vorderingen zoals bedoeld in artikel 3:305a lid 7 BW, welke aantekening vergezeld zal gaan van een afschrift van de Dagvaarding.

733. Conform artikel 1018c lid 3 Rv houdt de rechtbank, tenzij zij Stichting ICAM aanstonds niet ontvankelijk verklaart overeenkomstig artikel 1018c lid 2 Rv, de zaak aan totdat een termijn van drie maanden is verstreken na aantekening van de Dagvaarding in het register. Tenzij ingevolge

[321] *Kamerstukken II* 2016-2017, 34 608, nr. 3, p. 43.
[322] *Kamerstukken II* 2016-2017, 34 608, nr. 3, p. 43.

artikel 1018d lid 3 Rv deze termijn is verlengd of een andere collectieve vordering voor dezelfde gebeurtenis of gebeurtenissen is ingesteld, wordt na het verstrijken van de termijn de behandeling van de zaak voortgezet in de stand waarin zij zich bevindt.

734. Conform artikel 1018d lid 1 Rv, kan een rechtspersoon als bedoeld in artikel 3:305a BW binnen drie maanden na aantekening van de Dagvaarding in het register, een collectieve vordering instellen voor dezelfde gebeurtenis of gebeurtenissen als waarop deze collectieve vordering betrekking heeft, over gelijksoortige feitelijke en rechtsvragen, onder vermelding van de aantekening van de Dagvaarding in het register. De collectieve vordering wordt ingesteld bij dezelfde rechtbank als waar deze collectieve vordering is ingesteld.

735. Conform artikel 1018d lid 2 Rv, kan de rechtbank de bedoelde termijn van drie maanden met maximaal drie maanden verlengen indien binnen een maand na de aantekening van de Dagvaarding in het register een rechtspersoon als bedoeld in artikel 3:305a BW ter griffie heeft laten aantekenen dat hij een collectieve vordering wil instellen voor dezelfde gebeurtenis of gebeurtenissen als waarop deze collectieve vordering betrekking heeft, onder vermelding van de aantekening in het register, maar dat de termijn van drie maanden niet volstaat.

736. Conform artikel 1018d lid 3 Rv, worden, voor de toepassing van het eerste boek van Rv de overeenkomstig artikel 1018d Rv ingestelde collectieve vorderingen na inschrijving op de rol gezamenlijk behandeld als één zaak.

737. Conform artikel 1018e lid 1 Rv, zal de rechtbank uit de eisers die overeenkomstig artikel 1018c of 1018d Rv een collectieve vordering hebben ingesteld en voldoen aan de eisen voor ontvankelijkheid van artikel 3:305a BW, de meest geschikte eiser als exclusieve belangenbehartiger aanwijzen overeenkomst het bepaalde in art. 1018e Rv.

9.4.4 De vordering van Stichting ICAM c.s. is niet summierlijk ondeugdelijk

738. Uit de memorie van toelichting bij de WAMCA blijkt dat artikel 1018c lid 5 sub c Rv met grote terughoudendheid dient te worden toegepast:

> "Doel van de bepaling is om in uitzonderlijke gevallen een collectieve vordering al voor de inhoudelijke behandeling ervan van tafel te krijgen omdat deze niet deugt. Een voorbeeld zou kunnen zijn het geval dat een collectieve vordering wordt ingesteld voor de burgerlijke rechter terwijl overduidelijk is dat alleen de bestuursrechter over de vordering kan oordelen op basis van de regels voor de scheiding tussen de bestuursrechter en de burgerlijke rechter."[323]

739. Er is in de onderhavige zaak geen enkele reden om aan te nemen dat de vordering van Stichting ICAM ondeugdelijk zou zijn, summierlijk of anderszins.

[323] *Kamerstukken II*, 2016/2017, 34 608, nr. 3, p. 39;

10 TOELICHTING OP DE INCIDENTELE VERZOEKEN EN VORDERINGEN

740. Stichting ICAM stelt zich op het standpunt dat zij de feiten en gronden voor de schending van de AVG, de onrechtmatige daad en de inbreuken op specifieke zorgwetgeving door de Staat c.s. in deze Dagvaarding voldoende heeft onderbouwd. Echter, zij heeft nog niet kunnen vaststellen (i) van hoeveel Gedupeerden daadwerkelijk persoonsgegevens zijn ontvreemd of (ii) in hoeverre de Staat c.s. weten of vermoeden dat van meer Gedupeerden persoonsgegevens zijn ontvreemd dan van de groep van 1.250 personen die zij tot op heden hebben erkend, zoals door ongeoorloofd gebruik van de exportfunctionaliteit in HP Zone Lite (paragraaf 3.4).

741. Stichting ICAM heeft meerdere malen bij de Staat c.s. verzocht om informatie te verstrekken over onder andere de logging van gegevens in de GGD-systemen en het onderzoek op basis waarvan is vastgesteld dat de gegevens van 1.250 personen zijn ingezien en ontvreemd. Tot op heden is die informatie echter niet verstrekt (paragraaf 1.5 en **producties H.1 en H.2**).

742. Stichting ICAM stelt daarom een aantal verzoeken en incidentele vorderingen in, die erop gericht zijn meer duidelijkheid te verkrijgen over (de omvang en gevolgen van) het GGD-datalek. Stichting ICAM conformeert zich ten aanzien van haar incidentele vorderingen aan het procesverloop zoals wordt voorgeschreven door de WAMCA, waarbij de Dagvaarding op grond van artikel 1018c lid 7 Rv eerst drie maanden ingeschreven staat in het Centraal Register voor Collectieve Acties. Stichting ICAM verzoekt de rechtbank echter wel om over haar incidentele verzoeken en vorderingen te beslissen voorafgaand aan de inhoudelijke behandeling van de hoofdzaak. Stichting ICAM zou op basis van de informatie die wordt verkregen uit deze verzoeken en vorderingen namelijk tot de conclusie kunnen komen dat haar vorderingen in de hoofdzaak dienen te worden gewijzigd.

10.1 Bevel ex artikel 22 Rv (verzoek A)

743. Op grond van artikel 22 Rv kan de rechter in elke stand van de procedure bevelen dat nadere informatie wordt verstrekt door een of meer partijen. Een partij kan dit weigeren als sprake is van gewichtige redenen. Er zijn in dit geval geen gewichtige redenen op grond waarvan de Staat c.s. kunnen weigeren aan een bevel op grond van artikel 22 RV gehoor te geven, zoals uiteen zal worden gezet in paragraaf 10.2.4. Ingevolge hun verplichtingen onder de AVG en de waarheidsplicht ex. artikel 21 Rv zijn de Staat c.s. juist gehouden nadere informatie te verstrekken. Stichting ICAM verzoekt de rechtbank dan ook om de Staat c.s. op grond van artikel 22 Rv te bevelen de hieronder in paragraaf 10.2.1 opgesomde informatie in het geding te brengen. Zij verzoekt al hetgeen wordt besproken in paragraaf 10.2 als hier herhaald en ingelast te beschouwen.

10.2 Inzagevordering ex artikel 843a Rv (vordering B)

744. Voor het geval de rechtbank niet zou overgaan tot een bevel aan de Staat c.s. ex artikel 22 Rv, vordert Stichting ICAM – aldus voorwaardelijk - inzage en afschrift van bescheiden op grond van artikel 843a Rv. Artikel 843a Rv bepaalt dat eenieder die daarbij (i) een rechtmatig belang heeft, inzage, afschrift of uittreksel kan vorderen van (ii) bepaalde bescheiden (iii) aangaande een rechtsbetrekking waarin hij of zijn rechtsvoorgangers partij zijn, van degene die deze bescheiden te zijner beschikking of onder zijn berusting heeft. Volgens vaste rechtspraak moet het rechtmatig belang worden beoordeeld in samenhang met de bepaalde bescheiden. De bescheiden moeten zo concreet mogelijk worden omschreven zodat duidelijk is waarop aanspraak wordt gemaakt en getoetst kan worden of een rechtmatig belang bestaat bij die bescheiden. Het is niet nodig dat de bescheiden waarvan afgifte wordt gevorderd stuk voor stuk worden omschreven.[324]

10.2.1 Bepaalde bescheiden

745. Stichting ICAM vordert inzage in en afschrift van een beperkt aantal bescheiden, waarvan vaststaat dat ze bestaan en dat zij zich in het domein van de Staat c.s. bevinden. Deze zijn voldoende bepaald. Het betreft bescheiden die door de GGD'en specifiek zijn benoemd in hun Woo-besluiten en waarvan zij hebben besloten deze niet openbaar te maken en bescheiden die in Kamerstukken zijn genoemd. De bescheiden zijn zo concreet mogelijk omschreven en aangeduid, bevinden zich bij de Staat c.s. en zijn in tijd beperkt omdat zij verband houden met de coronapandemie en het GGD-datalek. Stichting ICAM vordert inzage in en afschrift van de volgende bescheiden (hierna de "**Bescheiden**"):

1) Logbestanden van activiteiten in CoronIT en HPZone Lite;[325]
2) Risicoanalyse uitgevoerd over de test- en traceerketen d.d. 22 december 2020;[326]
3) IT-assessment op het IT landschap van de COVID-19 bestrijding door GGD GHOR Nederland van december 2020;
4) IT-audit KPMG d.d. 18 december 2020;[327]
5) Analyse KPMG interne systemen d.d. 20 januari 2021; [328]
6) Rapportage functionele beveiligingstest uitgevoerd door Fox-IT; [329]
7) Extern onderzoek naar de kwaliteit van de software en de kwaliteit van de dienstverlening van de softwareleverancier van HPZone;[330]

---

[324] Hoge Raad 26 oktober 2012, ECLI:NL:HR:2012:BW9244 (*Eiser/Theodoor Gilissen Bankiers N.V.*), r.o. 3.8.2.
[325] Zie paragrafen 3.4 en 4.2.4.4.
[326] *Kamerstukken II* 2020-2021, 27 529, nr. 252.
[327] Feitenrelaas inzake gebeurtenissen omtrent coronatest-IT-systeem van de GGD, p. 6 (**productie D.6**).
[328] *Kamerstukken II* 2020-2021, 27 529, nr. 235, p. 9 (**productie D.3**)
[329] Door de Tweede Kamer ontvangen op 28 april 2021, zoals blijkt uit *Kamerstukken II* 2020-2021, 25295, nr. 1179, p. 41 (**productie D.9**).
[330] Stand van zakenbrief digitale ondersteuning pandemiebestrijding d.d. 12 februari 2021 (**productie D.7**).

8) Externe (technische en cultuur) audits genoemd in een Kamerbrief d.d. 23 maart 2021;[331]
9) Penetratietest Web Applicatie Omgeving voor het melden testresultaten;[332]
10) Overzicht maatregelen HPZone CoronIT GGD GHOR Nederland (20210129 overzicht maatregelen HP Zone CoronIT GGDGHOR NLv2.pdf);[333]
11) Presentatie NR - Acties ICT DATA (Acties nav datalek COVID 20210218);[334]
12) Projectplan Fase 2 DOTT[335]
13) Brief GGD GHOR Nederland aan gebruikers HPZone en HPZone Lite (brief GGD GHOR Ndl inz updates en queries in HPZone);[336]
14) Stand van Zaken HPZone;[337]
15) Brief t.a.v. portefeuillehouder en programmamanager testen;[338]
16) Analyse database HPZone;[339]
17) Oplegnotitie DPG-Raad Governancevoorstel HPZone;[340]
18) Governance beheer HPZone;[341]
19) Oplegnotitie Vervanging HP Zone (Lite) t.b.v. COVID-19 bestrijding;[342]
20) Memo toelichting op ontwikkelingen sinds 12 februari 2021;[343]
21) Rapportage KPMG Vervanging HPZone;[344]
22) Advies stuurgroep Transitie vervanging HPZone (Lite) t.b.v. covid 19 bestrijding;[345]
23) Advies afstemmingsoverleg IZB aan Stuurgroep Transitie 29 maart 2021;[346]
24) Governance Fase 1 uitfaseren HPZone (Lite);[347]
25) DPG-overleg 29.01.2021 besluitvorming HPZone;[348]
26) Oplegnotitie Governance vervanging HPZone (Lite) fase 1;[349]
27) Toelichting n.a.v. vragen Governance Fase 1.[350]

---

331 *Kamerstukken II* 2020-2021, 25 295, nr. 1063, p. 33.
332 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 5.1 (**productie I.9**).
333 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, p. 2 (**productie I.9**).
334 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, p. 2 (**productie I.9**).
335 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 10.4 (**productie I.9**).
336 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 10.8 (**productie I.9**).
337 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 10.9 (**productie I.9**).
338 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 10.14 (**productie I.9**).
339 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 10.15 (**productie I.9**).
340 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 11.1 (**productie I.9**).
341 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 11.2 (**productie I.9**).
342 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 12.1 (**productie I.9**).
343 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 12.3 (**productie I.9**).
344 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 12.4 (**productie I.9**).
345 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 12.5 (**productie I.9**).
346 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 12.6 (**productie I.9**).
347 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 12.7 (**productie I.9**).
348 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 12.8 (**productie I.9**).
349 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 12.9 (**productie I.9**).
350 GGD Zeeland, Inventarisatielijst bij deelbesluit I d.d. 1 juni 2022, document 12.10 (**productie I.9**).

10.2.2 Rechtmatig belang

746. Stichting ICAM heeft in het kader van een zorgvuldige en adequate belangenbehartiging belang bij inzage in en afschrift van de Bescheiden. Zij wenst daarmee informatie te verkrijgen over (het onderzoek naar) de omvang van de (verschillende categorieën binnen de) groep Gedupeerden. De Gedupeerden hebben er belang bij om te weten hoe groot het risico is dat hun gegevens zijn ontvreemd. Ook hebben zij er belang bij om vastgesteld te zien of hun gegevens al dan niet daadwerkelijk ontvreemd zijn, nu Stichting ICAM in deze procedure voor de groep personen van wie kan worden vastgesteld dat gegevens zijn ontvreemd een hogere schadevergoeding vordert. Op basis van de Bescheiden kan Stichting ICAM inzicht verkrijgen in het onderzoek dat is gedaan naar de omvang van deze groep personen. Uit de Bescheiden kan ook blijken of en hoe de logging in de GGD-systemen heeft plaatsgevonden.

10.2.3 Rechtsbetrekking

747. De rechtsbetrekking betreft een onrechtmatige daad door de Staat c.s., die bestaat uit een inbreuk op de persoonlijke levenssfeer van de Gedupeerden die door Stichting ICAM worden vertegenwoordigd op grond van artikel 3:305a BW. In hoofdstuk 9 wordt toegelicht dat Stichting ICAM voldoet aan de ontvankelijkheidseisen op grond van artikel 3:305a BW en de WAMCA. Op basis van het voorgaande is Stichting ICAM partij in de rechtsbetrekking en derhalve gerechtigd deze incidentele vordering tot afschrift en inzage in te stellen.

10.2.4 Geen gewichtige redenen

748. Op grond van artikel 843a lid 4 Rv kan degene die de beschikking heeft over de Bescheiden inzage en afgifte daarvan weigeren als (i) daarvoor gewichtige redenen bestaan en (ii) redelijkerwijs kan worden aangenomen dat een behoorlijke rechtsbedeling zonder verschaffing van de Bescheiden is gewaarborgd.

749. De Staat c.s. komt geen beroep toe op artikel 843a lid 4 Rv. Er zijn geen dringende redenen die aan verstrekking van de Bescheiden in de weg staan en een behoorlijke rechtsbedeling is zonder de Bescheiden niet gewaarborgd.

750. Voor zover de Staat c.s. zouden betogen dat het openbaar worden van de Bescheiden een risico zou opleveren voor de beveiliging van systemen (zoals door de GGD'en in hun Woo-besluiten wordt betoogd, zie paragraaf 1.5) en dat belang zou dienen te prevaleren boven het belang van Stichting ICAM bij verkrijging van de Bescheiden, gaat dat betoog niet op. Aan het belang van beveiliging van systemen en informatie kan immers tegemoet worden gekomen door met Stichting ICAM afspraken te maken over vertrouwelijkheid van bepaalde informatie, zoals de afspraak dat de documenten in eerste instantie alleen worden ingezien door de advocaten van partijen en een onafhankelijke derde, teneinde vervolgens te bepalen welke gedeelten vertrouwelijk moeten blijven en welke gedeelten niet.

751. Stichting ICAM benadrukt dat zij uitsluitend inzage en afschrift wil verkrijgen in de Bescheiden voor zover daaruit blijkt op welke wijze onderzoek is gedaan naar de omvang van het datalek en in hoeverre de Staat c.s. kunnen uitsluiten dat gegevens van meer dan 1.250 personen onbevoegd zijn ingezien en/of ontvreemd.

752. Stichting ICAM heeft, zoals in randnummers 740 t/m 742 hiervoor is beschreven, geen andere mogelijkheden om de Bescheiden te verkrijgen en vast te kunnen stellen wat de omvang van het datalek is. Inzage in en afschrift van in de Bescheiden is daardoor ook in het belang van een goede rechtsbedeling.

10.2.5 Procedure voor inzage in en afschrift van de Bescheiden

753. Stichting ICAM vordert primair om de Staat c.s. te bevelen om digitale afschriften van alle verzochte Bescheiden aan Stichting ICAM te verstrekken.

754. Subsidiair, voor het geval de rechtbank zou oordelen dat de vertrouwelijkheid van de Bescheiden of althans een deel daarvan daardoor onvoldoende gewaarborgd zou zijn, vordert Stichting ICAM om ten aanzien van die Bescheiden te bepalen dat digitale afschriften daarvan uitsluitend aan de advocaten van Stichting ICAM en aan een door de rechtbank te benoemen deskundige zullen worden verstrekt, waarbij door de Staat c.s. in ieder document gemotiveerd wordt aangegeven welke gedeelten vertrouwelijk zouden zijn. De deskundige zal vervolgens in samenspraak met de advocaten van Stichting ICAM en de advocaten van de Staat c.s. bepalen welke gedeelten vertrouwelijk moeten blijven en welke gedeelten niet. De documenten die in het geheel als vertrouwelijk worden aangemerkt blijven buiten beschouwing en de gedeelten in documenten die als vertrouwelijk worden aangemerkt, worden zwartgemaakt. Stichting ICAM vordert vervolgens om Stichting ICAM toestemming te verlenen om inzage te verkrijgen in en afschrift te verkrijgen van die selectie van de Bescheiden, zulks door te bepalen dat de Staat c.s. de selectie van Bescheiden, inclusief overeengekomen zwartmakingen, digitaal verstrekt aan Stichting ICAM. Teneinde de vertrouwelijkheid te waarborgen, vordert Stichting ICAM om te bepalen dat de deskundige en de advocaten van Stichting ICAM aan geheimhouding gebonden zijn ten aanzien van de als vertrouwelijk aangemerkte Bescheiden en de als vertrouwelijk aan te merken gedeelten van Bescheiden.

755. Meer-subsidiair vordert Stichting ICAM om de Staat c.s. te bevelen inzage in en afschrift van de Bescheiden te geven op een wijze door de rechtbank in goede justitie te bepalen.

10.3 Deskundigenonderzoek naar (de omvang en gevolgen van) het datalek (vordering C)

756. Ongeacht of de rechtbank het verzoek c.q. de vordering van Stichting ICAM ex artikel 22 Rv c.q. artikel 843a Rv toewijst, hebben de Gedupeerden, en daarmee Stichting ICAM, er belang bij dat

onafhankelijk en deskundig onderzoek wordt gedaan naar de omvang en risico's van het GGD-datalek. Tot op heden blijven de Staat c.s. vaag over de vraag of en in hoeverre kan worden uitgesloten dat van meer personen gegevens zijn ontvreemd dan van de groep van 1.250. Het is mogelijk dat er in het criminele circuit datasets circuleren van miljoenen mensen. Een deskundige kan onderzoeken of dat inderdaad het geval is en, voor zover dat niet sluitend kan worden vastgesteld, hoe groot het risico is dat dit het geval is. Op basis van de uitkomsten van dat onderzoek kunnen Gedupeerden geïnformeerd worden en zich beter wapenen tegen eventueel misbruik van hun gegevens. Daarom verzoekt Stichting ICAM de rechtbank om een deskundigenbericht te gelasten en de deskundige opdracht te geven tot een dergelijk onderzoek, zij het op basis van informatie die door de Staat c.s. wordt overgelegd op grond van het verzoek ex artikel 22 Rv en/of de vordering ex artikel 843a Rv dan wel uitsluitend op basis van eigen onderzoek.

10.4 Melding aan de Gedupeerden (vordering D)

757. Zoals toegelicht in paragraaf 4.2.3, zijn de Staat c.s. op grond van artikel 34 AVG verplicht om het GGD-datalek rechtstreeks te melden aan alle Gedupeerden, zowel de Gedupeerden Categorie A als de Gedupeerden Categorie B. Door de onduidelijke communicatie vanuit de Staat c.s. (paragraaf 3.4), verkeren miljoenen Gedupeerden momenteel in onzekerheid over de vraag of hun persoonsgegevens ontvreemd zijn of niet, of zelfs in de onterechte veronderstelling dat dat niet het geval is. Indien zij juist en volledig geïnformeerd worden over de kans dat hun gegevens in criminele handen terecht zijn gekomen, kunnen zij zich tegen eventueel misbruik van de gegevens beter wapenen. Er is daarom een groot belang bij dat de Gedupeerden op de kortst mogelijke termijn alsnog volledig en juist worden geïnformeerd over de risico's.

758. Stichting ICAM is van mening dat een rechtstreekse melding reeds had moeten plaatsvinden aan alle Gedupeerden, maar kan zich er vanwege het tijdsverloop dat inmiddels toch al heeft plaatsgevonden eventueel ook bij neerleggen dat deze melding pas wordt gedaan nadat meer duidelijkheid is verkregen over de vraag wat nu exact het risico is dat van meer personen gegevens zijn ontvreemd dan enkel van de groep van 1.250, en aldus nadat het deskundigenrapport is opgemaakt (paragraaf 3.4).

10.5 Beschikbaar houden van informatie en gegevens (vordering E)

759. De Gedupeerden hebben er belang bij dat informatie over het GGD-datalek en de risico's daarvan beschikbaar zijn en blijven, in ieder geval zolang deze procedure loopt. Op basis van deze informatie zal immers mogelijk onder andere dienen te worden bepaald welke personen recht hebben op schadevergoeding en hoe hoog deze schadevergoeding zal zijn per persoon. Ook is deze informatie nodig om met de Gedupeerden contact te kunne leggen over de uitkering van een schadevergoeding. Daarbij zijn niet alleen de NAW-gegevens relevant. Het is immers denkbaar dat komt vast te staan dat bijvoorbeeld (uitsluitend) inzake een specifieke periode, een

specifiek IT-systeem of een specifieke categorie Gedupeerden sprake is van een (voldoende ernstige) schending van de AVG en aldus van aansprakelijkheid en een verplichting tot vergoeding van schade. In dat geval is van belang dat vastgesteld kan worden welke gegevens van welke Gedupeerden gedurende welke (deel)periode in welk (deel van een) systeem opgenomen zijn (geweest). Indien de Gedaagden gegevens verwijderen kan dat ertoe leiden dat de Gedupeerden niet kunnen aantonen dat hun persoonsgegevens in strijd met de AVG zijn verwerkt. Dat kan ertoe leiden dat zij hun recht op schadevergoeding niet kunnen effectueren. Stichting ICAM vordert daarom om de Staat c.s. te bevelen om bepaalde informatie te bewaren en beschikbaar te houden voor deze doelen.

10.6 Veroordeling in de kosten van het incident (vordering F)

760. De incidentele verzoeken en vorderingen van Stichting ICAM zijn verbonden aan de vorderingen in de hoofdzaak, nu zij ertoe strekken Stichting ICAM en de Gedupeerden van nadere informatie te voorzien omtrent de omvang en gevolgen van het GGD-datalek. De Staat c.s. is daarom op grond van artikel 1018l lid 2 Rv gehouden de kosten die verband houden met de ingestelde incidentele vorderingen te dragen. Het gaat daarbij in ieder geval om de redelijke en evenredige gerechtskosten en andere kosten van het incident, waaronder de (nader te begroten) kosten die verbonden zijn aan het verkrijgen van inzage, afschrift of uittreksel en waaronder de advocaatkosten en de kosten voor de deskundige(n).

10.7 Dwangsommen (vordering G)

761. De oplegging van dwangsommen aan de Staat c.s. is naar overtuiging van Stichting ICAM noodzakelijk om te bewerkstelligen dat de Staat c.s. tijdig en volledig voldoen aan de verplichtingen die voor hen voortvloeien uit het in het incident te wijzen vonnis. Dat er aanleiding en noodzaak bestaat om de Staat c.s. dwangsommen op te leggen, blijkt ten aanzien van artikel 843a Rv bijvoorbeeld uit het feit dat de Staat c.s. in de Woo-procedures niet bereid is de gevraagde Bescheiden aan Stichting ICAM ter beschikking te stellen (zie ook paragraaf 10.2.1). Bovendien hebben de Staat c.s. tot op heden geen melding gedaan van het GGD-datalek aan alle Gedupeerden. Ook dat maakt dat er aanleiding is om nakoming van de verplichtingen van de Staat c.s. te verzekeren middels oplegging van dwangsommen.

11 TOELICHTING OP DE VORDERINGEN IN DE HOOFDZAAK

11.1 Stichting ICAM als Exclusieve Belangenbehartiger (vordering H)

762. Voor een toelichting op deze vordering verwijst Stichting ICAM naar paragraaf 9.4.2. Stichting ICAM is uiteraard bereid nader toe te lichten waarom zij het best geplaatst is de belangen van de Gedupeerden te behartigen en verzoekt de rechtbank haar gelegenheid te geven dat te doen indien de rechtbank niet direct tot benoeming van Stichting ICAM zou overgaan.

11.2 De vertegenwoordigde groep personen (vordering I)

763. Voor een toelichting op deze vordering verwijst Stichting ICAM naar paragraaf 9.1.3.1.

11.3 Opt-out / Opt-in (vordering J)

764. Op grond van artikel 1018f lid 1 Rv kunnen personen behorend tot de nauw omschreven groep personen wier belangen in de collectieve vordering worden behartigd, binnen een door de rechtbank te bepalen termijn van minstens een maand na aankondiging van de uitspraak bedoeld in artikel 1018e lid 1 en 2 Rv laten weten dat zij zich van de behartiging van hun belangen in de collectieve vordering willen bevrijden (het opt-out-recht).

765. Stichting ICAM meent dat het in deze zaak noodzakelijk is om een termijn van drie maanden te bepalen voor het inroepen van het opt-out-recht, dit vanwege de omvang en diversiteit van de groep Gedupeerden. Iedere Gedupeerde dient een redelijke gelegenheid te hebben om kennis te nemen van de uitspraak en om de gevolgen van deze collectieve vordering voor zijn persoonlijke situatie te beoordelen. Een termijn van een maand is daarvoor onvoldoende. Om dezelfde reden vordert Stichting ICAM om de Gedaagden te bevelen de uitspraak te laten vertalen in de meest gesproken vreemde talen in Nederland en de uitspraak aan te kondigen in alle landelijke en regionale dagbladen.

766. Op grond van artikel 1018f lid 5 Rv kunnen personen behorend tot de nauw omschreven groep personen wier belangen in de collectieve vordering worden behartigd, maar die geen woonplaats of verblijf in Nederland hebben, binnen een door de rechtbank te bepalen termijn van minstens een maand na aankondiging van de uitspraak bedoeld in artikel 1018e lid 1 en 2 Rv laten weten dat zij juist wel instemmen met de behartiging van hun belangen in de collectieve vordering (het opt-in-recht). De laatste zin van dit artikellid bepaalt dat op verzoek van een partij de rechter bepalen dat, in afwijking van dit lid, het eerste lid van artikel 1018f Rv (het opt-out-recht) van toepassing is op personen behorend tot de nauw omschreven groep personen wier belangen in de collectieve vordering worden behartigd en die geen woonplaats of verblijf in Nederland hebben.

767. Stichting ICAM verzoekt de rechtbank primair om van deze bevoegdheid gebruik te maken aangezien dit een relatief kleine groep personen zal betreffen die zich hebben laten testen of vaccineren in Nederland, maar niet of inmiddels niet meer wonen. Er is geen reden om deze personen buiten de nauw omschreven groep te houden. Subsidiair acht Stichting ICAM voor deze personen een termijn van zes maanden noodzakelijk om hun opt-in-recht uit te oefenen. Nu dit een relatief kleine groep personen zal betreffen die in ieder geval enige band met Nederland hebben, acht Stichting ICAM het niet noodzakelijk om daarvoor andere aankondigingen te doen dan zoals reeds hierboven besproken.

768. Om ook Gedupeerden te bereiken die de Nederlandse taal niet goed beheersen, vordert Stichting ICAM om de Staat c.s. te bevelen om de communicatie over het opt-out-recht en opt-in-recht aan te bieden in ten minste dezelfde talen als waarin de website www.prikkenzonderafspraak.nl van de Rijksoverheid wordt aangeboden, zijnde op de datum van dagvaarding Nederlands, Engels, Turks, Pools en Arabisch.

11.4 Verklaringen voor recht (vordering K)

769. Stichting ICAM en de Gedupeerden hebben er belang bij dat met een verklaring voor recht wordt vastgesteld dat de Staat c.s. in strijd met de AVG en onrechtmatig hebben gehandeld, en dat zij aansprakelijk zijn voor de daardoor veroorzaakte schade. Dit belang komt onder meer voort uit het risico dat Stichting ICAM onverhoopt niet ontvankelijk wordt verklaard of dat haar collectieve vorderingen worden afgewezen. De Gedupeerden kunnen dan alsnog besluiten zelf individuele procedures te voeren.

11.5 Beëindigen van de inbreuk en verbeteren van beveiligingsmaatregelen (vordering L)

770. Stichting ICAM vordert vanzelfsprekend dat de Staat c.s. worden bevolen om hun AVG-overtredingen en hun onrechtmatig handelen te staken en gestaakt te houden, onder meer door in zijn algemeenheid betere gegevensbeveiliging na te streven.

11.6 Schadevergoeding (vorderingen M en N)

771. Over de vordering tot schadevergoeding heeft Stichting ICAM in het voorgaande al voldoende toegelicht (paragrafen 5.3 en 5.4).

11.7 Kostenvergoedingen (vordering O)

772. De Staat c.s. dient uit hoofde van artikel 1018l lid 2 Rv veroordeeld te worden in de kosten van dit geding. Artikel 1018l lid 2 geeft de mogelijkheid een kostenveroordeling uit te spreken die – anders dan artikel 237 Rv - afwijkt van het liquidatietarief in het geval een collectieve schadeafwikkeling (ex artikel 1018i Rv) wordt vastgesteld. Stichting ICAM maakt dan ook aanspraak op de volledige door haar gemaakte buitengerechtelijke kosten, de redelijke en evenredige gerechtskosten en andere kosten. Dat houdt mede in dat Stichting ICAM aanspraak maakt op betaling van de aan de Financier uit hoofde van de Financieringsovereenkomst verschuldigde vergoeding, zijnde twintig procent van (enig gedeelte van) ieder geldbedrag, dan wel ieder op geld waardeerbaar goed, dat op grond van de vorderingen daadwerkelijk aan de Gedupeerden wordt toegekend. Dat laatste zorgt ervoor dat de volledige vergoeding die aan de Gedupeerden toegewezen wordt, hen ook daadwerkelijk ten gunste komt.

11.8 Schadeafwikkeling (vordering P)

773. De schadeafwikkeling in deze omvangrijke zaak kan niet anders verlopen dan door het inschakelen van een deskundige en ervaren partij op dit gebied, waarbij een vergaande medewerking van de Gedaagden noodzakelijk is. Vordering P is daarop gericht. Stichting ICAM verzoekt de rechtbank haar toe te staan zich over de identiteit van de deskundige partij nog uit te laten.

11.9 Dwangsommen (vorderingen Q)

774. Stichting ICAM acht het noodzakelijk om dwangsommen te verbinden aan haar verzoeken c.q. vorderingen voor het geval de Staat c.s. hun verplichtingen uit hoofde van het te dezen te wijzen vonnis niet (tijdig en/of volledig) nakomen. Het opleggen van dwangsommen vormt een stimulans voor de Staat c.s. om tijdig en volledig aan hun verplichtingen te voldoen en leidt tot zekerheid voor Gedupeerden dat de Staat c.s. daadwerkelijk over zullen gaan tot het beëindigen van de inbreuk en het doorvoeren van verbetermaatregelen. Nu de Staat c.s. de inbreuk nog steeds niet beëindigd hebben en ook geen afdoende verbetermaatregelen hebben doorgevoerd, bestaat er aanleiding om dwangsommen op te leggen.

12 PETITUM

775. Dat het de rechtbank moge behagen om bij vonnis, voor zover mogelijk uitvoerbaar bij voorraad:

IN HET INCIDENT

A Verzoek tot een bevel ex artikel 22 Rv

A.I De Staat c.s. op grond van artikel 22 Rv te bevelen om de in paragraaf 10.2.1 opgesomde informatie en/of documenten in het geding te brengen.

B Voorwaardelijke vordering: inzage en afschrift ex artikel 843a Rv

Indien of voor zover de rechtbank verzoek A niet honoreert:

Primair

B.I Gedaagden te bevelen om binnen tien (10) dagen na betekening van het vonnis in incident een digitaal afschrift van de Bescheiden (zoals genoemd in paragraaf 10.2.1 van deze Dagvaarding) te verstrekken aan Stichting ICAM.

Subsidiair

B.II Gedaagden te bevelen om binnen tien (10) dagen na betekening van het vonnis in incident een digitaal afschrift van de Bescheiden te verstrekken aan de advocaten van Stichting ICAM en aan een door de rechtbank te benoemen deskundige, waarbij door Gedaagden ten aanzien van ieder document gemotiveerd wordt aangegeven welk onderdeel of welke onderdelen vertrouwelijk zouden zijn, waarna de deskundige in samenspraak met de advocaten van Stichting ICAM en de advocaten van de Gedaagden zal bepalen welke bescheiden of gedeelten van bescheiden vertrouwelijk moeten blijven en welke documenten of gedeelten niet, waarbij als vertrouwelijk aangemerkte Bescheiden vernietigd zullen worden en als vertrouwelijk aan te merken gedeelten van Bescheiden zullen worden zwartgemaakt.

B.III Daarbij te bepalen dat de deskundige en de advocaten van Stichting ICAM aan geheimhouding gebonden zijn ten aanzien van de als vertrouwelijk aangemerkte Bescheiden en de als vertrouwelijk aan te merken gedeelten van Bescheiden.

B.IV Te bepalen dat indien de deskundige, de advocaten van Stichting ICAM en de advocaten van Gedaagden niet tot overeenstemming komen over de vraag welke gedeelten vertrouwelijk moeten blijven en welke gedeelten niet, de deskundige hierover bindend zal besluiten.

B.V Te bepalen dat de deskundige binnen vijf (5) dagen na voltooiing van de door hem of haar te plegen vaststelling een digitaal afschrift van de Bescheiden, met uitzondering van hetgeen als vertrouwelijk is aangemerkt, zal verstrekken aan Stichting ICAM.

Meer-subsidiair

B.VI Gedaagden te bevelen om binnen tien (10) dagen na betekening van het vonnis in incident inzage, afschrift of uittreksel van de Bescheiden te verstrekken aan Stichting ICAM op een wijze zoals door de rechtbank in goede justitie te bepalen.

C Deskundigenonderzoek naar (de omvang en gevolgen van) het datalek

C.I Een door de rechtbank te benoemen deskundige opdracht te geven om in overleg met Gedaagden en Stichting ICAM te onderzoeken wat de omvang en risico's van het datalek zijn, althans zijn geweest, met inbegrip van de vraag van hoeveel en van welke (categorieën van) personen persoonsgegevens uit de GGD-systemen onbevoegd konden worden, zijn en/of kunnen worden ingezien en/of ontvreemd, zulks met opdracht aan de deskundige om binnen acht (8) weken na het vonnis in incident van zijn of haar bevindingen schriftelijk en gedetailleerd verslag te doen aan de rechtbank en Stichting ICAM.

C.II Gedaagden te bevelen om aan het onderzoek van en de rapportage door de deskundige volledig en onvoorwaardelijk medewerking te verlenen en aan de deskundige alle informatie te verschaffen die de deskundige relevant acht voor de uitvoering van zijn of haar onderzoek.

D Melding aan Gedupeerden

D.I Gedaagden te bevelen om binnen vier (4) weken na betekening van het vonnis in incident, althans binnen vier (4) weken na het beschikbaar komen van het in vordering C bedoelde rapport, alle Gedupeerden van wie persoonsgegevens in de GGD-systemen onbevoegd konden worden, zijn en/of kunnen worden ingezien en/of ontvreemd, hierover zoveel mogelijk op individuele basis schriftelijk te informeren, onder vermelding van de (mogelijke) gevolgen en risico's daarvan, en om van die informatieverschaffing binnen twee (2) weken na het informeren van de Gedupeerden schriftelijk en gedetailleerd verslag te doen aan de rechtbank.

E Beschikbaar houden van gegevens

E.I Gedaagden te bevelen om, ieder voor zover zij hierover beschikken, de hierna genoemde informatie en gegevens van alle Gedupeerden te bewaren en beschikbaar te houden voor zolang dat nodig is (i) om tot volledige en correcte melding aan de Gedupeerden over te gaan zoals bedoeld in vordering D en (ii) om tot volledige en correcte uitbetaling van schadevergoeding over te kunnen gaan:

a) Voor- en achternaam;
b) Geboortedatum;
c) Adres;
d) E-mailadres en telefoonnummer;
e) De gegevens die onbevoegd konden worden, zijn en/of kunnen worden ingezien en/of ontvreemd;
f) De periode waarin de betreffende gegevens onbevoegd konden worden, zijn en/of kunnen worden ingezien en/of ontvreemd;
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 gestolen of anderszins zijn aangewend op een wijze die tot aansprakelijkheid van Gedaagden jegens Gedupeerden leidt;
i) Logbestanden.

E.II Een door de rechtbank te benoemen deskundige opdracht te geven om periodiek te controleren of (blijvend) aan het bevel op grond van vordering E.I wordt voldaan, zulks met opdracht aan de deskundige om van zijn of haar bevindingen iedere drie (3) maanden schriftelijk en gedetailleerd verslag te doen aan de rechtbank en Stichting ICAM.

E.III Gedaagden te bevelen om aan het onderzoek van en de rapportage door de deskundige volledig en onvoorwaardelijk medewerking te verlenen en aan de deskundige alle informatie te verschaffen die de deskundige relevant acht voor de uitvoering van zijn of haar onderzoek.

F Kostenvergoeding

F.I Gedaagden op de voet van 1018l lid 2 Rv hoofdelijk te veroordelen in de redelijke en evenredige gerechtskosten en andere kosten van het incident, waaronder de nader te begroten kosten verbonden aan het verkrijgen van inzage, afschrift of uittreksel en waaronder de advocaatkosten en de kosten voor de deskundige(n).

G Dwangsommen

G.I Gedaagden hoofdelijk te bevelen een dwangsom te betalen van € 250.000,- (zegge: tweehonderdenvijftigduizend euro) voor iedere dag (een gedeelte van een dag als een gehele gerekend) dat zij geheel of gedeeltelijk in strijd handelen met de bevelen op grond van de verzoeken c.q. vorderingen A, B, C.II, D en/of E, met een maximum van € 100.000.000,- (zegge honderd miljoen euro).

IN DE HOOFDZAAK

H Exclusieve belangenbehartiger

H.I Stichting ICAM aan te wijzen als exclusieve belangenbehartiger in de zin van artikel 1018e lid 1 Rv.

I De vertegenwoordigde groep personen

I.I In het kader van artikel 1018e lid 2 Rv te bepalen dat Stichting ICAM in deze collectieve vordering de belangen behartigt van alle Gedupeerden, zijnde:

a) Alle natuurlijke personen van wie persoonsgegevens zijn verwerkt in één van of beide GGD-systemen in de periode tussen ingebruikname daarvan in verband met de bestrijding van corona en 1 februari 2021, bijvoorbeeld omdat zij een afspraak hebben gemaakt bij een GGD om te testen of vaccineren in verband met corona of omdat zij onderdeel zijn geweest van bron- en contactonderzoek in verband met corona, met uitzondering van de personen die deel uitmaken van Gedupeerden Categorie B (“Gedupeerden Categorie A”)

b) Alle natuurlijke personen van wie persoonsgegevens zijn verwerkt in één van of beide GGD-systemen in de periode tussen ingebruikname daarvan in verband met de bestrijding van corona en 1 februari 2021, bijvoorbeeld omdat zij een afspraak hebben gemaakt bij

een GGD om te testen of vaccineren in verband met corona of omdat zij onderdeel zijn geweest van bron- en contactonderzoek in verband met corona, en waarvan vaststaat of zal worden vastgesteld dat hun persoonsgegevens als gevolg van het GGD-datalek door ongeautoriseerde personen zijn ingezien of bij ongeautoriseerde personen in handen zijn gekomen, zoals door het ongeoorloofd inzien, downloaden, exporteren, printen, kopiëren, fotograferen en/of aanbieden, verhandelen, ontvangen of op andere wijze delen van de persoonsgegevens ("Gedupeerden Categorie B").

J Opt-out / Opt-in

J.I Gedaagden te bevelen om de uitspraak op grond van artikel 1018e lid 1 en 2 Rv, vergezeld van een eenvoudige samenvatting, alsmede vertalingen van de uitspraak en de samenvatting in tenminste dezelfde talen als waarin de website www.prikkenzonderafspraak.nl van de Rijksoverheid wordt aangeboden, binnen vier (4) weken na de datum van de uitspraak te plaatsen op (i) de website van GGD GHOR, (ii) de websites van de GGD'en en (iii) een speciaal daarvoor in het leven te roepen website van de Rijksoverheid, zodanig dat deze door de Gedupeerden ten behoeve van latere kennisneming kunnen worden opgeslagen.

J.II Gedaagden te bevelen om binnen vier (4) weken na de datum van de uitspraak op grond van artikel 1018e lid 1 en 2 Rv alle Gedupeerden bij gewone brief mededeling te doen van de aanwijzing van de Exclusieve Belangenbehartiger, de collectieve vordering en de nauw omschreven groep personen wier belangen de Exclusieve Belangenbehartiger in deze collectieve vordering behartigt.

J.III Gedaagden te bevelen om binnen vier (4) weken na de datum van de uitspraak op grond van artikel 1018e lid 1 en 2 Rv aankondiging te doen van de aanwijzing van de Exclusieve Belangenbehartiger en de collectieve vordering en de nauw omschreven groep personen wier belangen de Exclusieve Belangenbehartiger in deze collectieve vordering behartigt, zulks in alle landelijke en regionale nieuwsbladen van Nederland en met een inhoud en op een wijze zoals door de rechtbank in goede justitie te bepalen na uitlating van partijen daarover.

J.IV Te bepalen dat (de wettelijk vertegenwoordiger(s) van) iedere persoon met woonplaats of verblijf in Nederland die behoort tot de groep Gedupeerden, gedurende een periode van drie (3) maanden na de aankondiging in de zin van artikel 1018f lid 3 Rv de mogelijkheid heeft om door middel van een schriftelijke mededeling aan de griffie van de rechtbank te laten weten zich van de behartiging van zijn of haar belangen in deze collectieve vordering te willen bevrijden (Opt-out).

J.V Te bepalen dat (de wettelijk vertegenwoordiger(s) van) iedere persoon zonder woonplaats of verblijf in Nederland die behoort tot de groep Gedupeerden, gedurende een periode van zes (6) maanden na de aankondiging in de zin van artikel 1018f lid 3 Rv de mogelijkheid heeft om door

middel van een schriftelijke mededeling aan de griffie van de rechtbank te laten weten in te stemmen met de behartiging van zijn of haar belangen in deze collectieve vordering (Opt-in).

K Verklaringen voor recht

K.I Voor recht te verklaren dat de Gedaagden ieder voor zich zelfstandig dan wel gezamenlijk met één of meer andere Gedaagden, in de zin van de AVG moeten worden aangemerkt als verwerkingsverantwoordelijken voor de gegevensverwerkingen in de GGD-systemen CoronIT en/of HPZone Lite.

K.II Voor recht te verklaren dat de Gedaagden, althans de als verwerkingsverantwoordelijken aan te merken Gedaagden, in strijd handelen met, althans in strijd hebben gehandeld met:

a) Artikel 8 EVRM; en/of
b) Artikel 7 Handvest; en/of
c) Artikel 8 Handvest; en/of
d) Artikel 5 AVG; en/of
e) Artikel 24 AVG; en/of
f) Artikel 25 AVG; en/of
g) Artikel 32 AVG; en/of
h) Artikel 34 AVG; en/of
i) Artikel 35 AVG; en/of
j) Artikel 7:457 BW; en/of
k) Artikel 10 Wabvpz jo. artikel 2 Regeling gebruik burgerservicenummer in de zorg; en/of
l) Artikel 15j Wabvpz jo. artikel 3 en 5 Begz.

K.III Voor recht te verklaren dat de Gedaagden jegens de Gedupeerden onrechtmatig handelen, althans onrechtmatig hebben gehandeld op grond van artikel 6:162 BW.

K.IV Voor recht te verklaren dat de Gedaagden, althans de als verwerkingsverantwoordelijken aan te merken Gedaagden, op grond van artikel 82 AVG en/of artikel 6:162 BW hoofdelijk aansprakelijk zijn voor alle schade die door de Gedupeerden is geleden en nog zal worden geleden ten gevolge van het GGD-datalek.

L Beëindigen van de inbreuk en verbeteren van beveiligingsmaatregelen

L.I Gedaagden, althans de als verwerkingsverantwoordelijken aan te merken Gedaagden, te bevelen om binnen drie maanden na het in deze zaak te wijzen vonnis alle in het lichaam van deze Dagvaarding omschreven inbreuken op het EVRM, het Handvest, de AVG en specifieke zorgwetgeving en al het in het lichaam van deze Dagvaarding omschreven onrechtmatig handelen, te staken en gestaakt te houden.

L.II De betreffende Gedaagden te bevelen om mee te werken aan beoordeling en controle van alle genomen maatregelen ter uitvoering van het bevel op grond van vordering L.I door een door de rechtbank aan te wijzen deskundige, zulks met opdracht aan de deskundige om binnen zes maanden na het in deze zaak te wijzen vonnis van zijn of haar bevindingen schriftelijk en gedetailleerd verslag te doen aan Stichting ICAM.

M Immateriële schadevergoeding

Primair

M.I Gedaagden hoofdelijk te veroordelen tot vergoeding van de immateriële schade van iedere Gedupeerde en die immateriële schade te begroten op:

a) Een bedrag van € 500,- (zegge: vijfhonderd euro) per Gedupeerde binnen Gedupeerden Categorie A;

b) Een bedrag van € 1.500,- (zegge: vijftienhonderd euro) per Gedupeerde binnen Gedupeerden Categorie B;

te vermeerderen met de wettelijke rente vanaf de datum van het in deze zaak te wijzen vonnis tot aan de dag der algehele voldoening.

Subsidiair

M.II Gedaagden hoofdelijk te veroordelen tot vergoeding van de immateriële schade van iedere Gedupeerde en die immateriële schade te begroten op een bedrag of bedragen door de rechtbank in goede justitie te bepalen, te vermeerderen met de wettelijke rente vanaf de datum van het in deze zaak te wijzen vonnis tot aan de dag der algehele voldoening.

Meer-subsidiair

M.III Te bepalen dat de door de Gedupeerden geleden immateriële schade nader zal worden opgemaakt bij staat en zal worden vereffend volgens de wet.

N Materiële schadevergoeding

Primair

N.I Gedaagden hoofdelijk te veroordelen tot vergoeding van de materiële schade van iedere Gedupeerde en die materiële schade te begroten op een bedrag van € 50,- (zegge: vijftig euro) per Gedupeerde, te vermeerderen met de wettelijke rente vanaf de datum van het in deze zaak

te wijzen vonnis tot aan de dag der algehele voldoening, met bepaling dat dit onverlet laat dat de Gedupeerden individueel gerechtigd zijn tot een hogere vergoeding voor materiële schade indien op enig moment blijkt dat die hoger is.

Subsidiair

N.II Een bedrag of bedragen door de rechtbank in goede justitie te bepalen, te vermeerderen met de wettelijke rente vanaf de datum van het in deze zaak te wijzen vonnis tot aan de dag der algehele voldoening, met bepaling dat dit onverlet laat dat de Gedupeerden individueel gerechtigd zijn tot een hogere vergoeding voor materiële schade indien op enig moment blijkt dat die hoger is.

Meer-subsidiair

N.III Te bepalen dat de door de Gedupeerden geleden materiële schade nader zal worden opgemaakt bij staat en zal worden vereffend volgens de wet.

O Kostenvergoedingen

Primair

O.I Gedaagden hoofdelijk te veroordelen tot vergoeding aan Stichting ICAM van:

a) De volledige door Stichting ICAM gemaakte buitengerechtelijke kosten;

b) De redelijke en evenredige gerechtskosten en andere kosten van Stichting ICAM, de nakosten daaronder begrepen, zulks op grond van artikel 1018l lid 2 Rv, althans artikel 237 Rv;

c) Indien of voor zover dit niet onder sub b) valt, de volledige door Stichting ICAM aan de Financier op grond van de Financieringsovereenkomst te betalen vergoeding, zijnde 20% (zegge: twintig procent) van (enig gedeelte van) ieder geldbedrag, dan wel ieder op geld waardeerbaar goed, dat op grond van de vorderingen daadwerkelijk aan de Gedupeerden wordt toegekend, met een maximum van een bedrag ter hoogte van vijfmaal het volledige bedrag dat daadwerkelijk door de Financier is geïnvesteerd ter financiering van deze procedure, een en ander te vermeerderen met BTW indien van toepassing;

een en ander zoals nader te begroten op basis van door Stichting ICAM over te leggen informatie en te vermeerderen met de wettelijke rente vanaf de datum van het in deze zaak te wijzen vonnis tot aan de dag der algehele voldoening, zo nodig op te maken bij staat en te vereffenen volgens de wet;

d) De volledige kosten van Stichting ICAM die zij nog zal maken in verband met de uitvoering van het in deze zaak te wijzen vonnis en de afhandeling van de vaststelling en uitbetaling van de schadevergoeding en de begeleiding van en controle op dat proces, conform de in vordering P bedoelde wijze van schadeafwikkeling, te vermeerderen met BTW indien van toepassing, steeds halfjaarlijks vooraf te voldoen op basis van door Stichting ICAM vast te stellen redelijke voorschotbedragen en na afronding af te rekenen op basis van nacalculatie.

Subsidiair

O.II Te bepalen dat Stichting ICAM de kosten zoals bedoeld in vordering O.I in mindering zal mogen brengen op de door of namens haar aan de Gedupeerden uit te betalen schadevergoedingen.

P Schadeafwikkeling

Primair

P.I Een door de rechtbank te benoemen deskundige op het vlak van de uitvoering en afhandeling van collectieve schadeafwikkeling opdracht te geven om in overleg met Gedaagden en Stichting ICAM tot de inning en verdeling van alle in deze procedure toegekende schadevergoedingen over te gaan.

P.II Gedaagden hoofdelijk te bevelen om binnen een maand na het in deze zaak te wijzen vonnis over te gaan tot voldoening van de bedragen bedoeld in vorderingen M en N op een door de deskundige daartoe specifiek in te richten kwaliteitsrekening.

P.III Gedaagden te bevelen volledig en onvoorwaardelijk medewerking te verlenen aan de schadeafwikkeling door de deskundige conform door de deskundige te geven instructies en aan de deskundige alle informatie te verschaffen die de deskundige relevant acht voor de uitvoering van zijn of haar taken in dat verband.

P.IV Gedaagden hoofdelijk te bevelen om de kosten die gemoeid zijn met de werkzaamheden van de deskundige, alsmede alle bijkomende kosten, te vermeerderen met BTW indien van toepassing, te vergoeden, steeds halfjaarlijks vooraf te voldoen op basis van de deskundige vast te stellen redelijke voorschotbedragen en na afronding af te rekenen op basis van nacalculatie.

P.V Te bepalen dat enig bedrag aan schadevergoeding dat na afhandeling van de schadeafwikkeling nog resteert en niet aan de Gedupeerden kan worden uitbetaald, door de deskundige zal worden uitgekeerd aan één of meer door Stichting ICAM aan te wijzen organisaties zonder winstoogmerk die actief zijn op het gebied van privacybescherming en beveiliging van persoonsgegevens.

P.VI Te bepalen dat de Gedupeerden die in aanmerking wensen te komen voor betaling van schadevergoeding, daarvoor dienen in te stemmen met een bindendadviesprocedure met betrekking tot de vaststelling door de deskundige van het recht op schadevergoeding en met betrekking tot de verdeling van de schadevergoeding, waarbij een door de rechtbank, na uitlating daarover door Stichting ICAM en Gedaagden, aan te wijzen onafhankelijke persoon met voldoende deskundigheid als bindend adviseur zal optreden.

Subsidiair

P.VII De collectieve schadeafwikkeling zodanig vorm te geven als de rechtbank geraden acht op basis van (een) door Stichting ICAM en/of Gedaagden op grond van artikel 1018i Rv over te leggen voorstel(len) voor een collectieve schadeafwikkeling.

Q Dwangsommen

Q.I Gedaagden hoofdelijk te bevelen een dwangsom te betalen van € 250.000,- (zegge: tweehonderdenvijftigduizend euro) voor iedere dag (een gedeelte van een dag als een gehele gerekend) dat zij geheel of gedeeltelijk in strijd handelen met de bevelen op grond van vordering J, L, P.II en/of P.III, met een maximum van € 100.000.000,- (zegge: honderd miljoen euro).

De kosten dezes van mij deurwaarder bedragen:

Deurwaarder

Deze zaak wordt behandeld door:
SOLV Advocaten
mr. D.M. Linders
mr. Y. van den Winkel
mr. A.L.M. Bakhuis
T: 020-5300160 I F: 020-5300170 I E: linders@solv.nl I E: winkel@solv.nl I E: bakhuis@solv.nl
Anne Frankstraat 121, 1018 BZ Amsterdam

INVENTARISLIJST PRODUCTIES BIJ DAGVAARDING (28 MAART 2023)

Categorie A Definities en afkortingen

A.1 Definities en afkortingen

Categorie B Stukken met betrekking tot Stichting ICAM

B.1 Statuten Stichting ICAM

B.2 Claimcode 2019

B.3 Screenshots www.datalek-ggd.nl

B.4 Screenshots www.stichtingicam.nl

B.5 Blogs en updates website

B.6 Updatemails aan de Deelnemers

B.7 Mediaberichten over ICAM en de collectieve actie

B.8 Verantwoordingsdocument wet en Claimcode

B.9 Verantwoordingsdocument Raad van toezicht d.d. 14 juli 2022

B.10 Bestuursverslag d.d. 14 juli 2022

B.11 Deelnemersovereenkomst versie december 2021

B.12 Deelnemersovereenkomst versie februari 2022

B.13 Flyer Stichting ICAM

Categorie C Nieuwsberichten

C.1 Nieuwsuur, 'Testlijnmedewerkers kunnen bij persoonsgegevens, ook als dat niet mag', www.nos.nl, 16 september 2020

C.2 RTV Oost, 'Datalek coronacallcenter, Steenwijker kon alle dossiers wekenlang inzien', www.rtvoost.nl, 16 september 2020

C.3 Trouw, 'Autoriteit Persoonsgegevens onderzoekt datalek bij GGD-testlijn. Wie kon privacygevoelige informatie inzien?', www.trouw.nl, 9 oktober 2020

C.4 Algemeen Dagblad, ‘GGD-medewerkers gluurden ongeoorloofd naar BN’ers in coronadatabase’, www.ad.nl, 3 november 2020

C.5 Volkskrant, 'Met dit houtje-touwje-systeem gaven GGD-medewerkers de coronacijfers door tot het crashte’, www.volkskrant.nl, 12 november 2020

C.6 RTL, 'Illegale handel in privégegevens miljoenen Nederlanders uit coronasystemen GGD', www.rtl.nl, 25 januari 2021

C.7 Autoriteit Persoonsgegevens, 'AP slecht bereikbaar door vragen datadiefstal GGD', www.autoriteitpersoonsgegevens.nl, 27 januari 2021

C.8 RTL, 'Privacylek coronasystemen was al maanden bekend, GGD deed niets, 'We konden overal bij'', www.rtl.nl, 28 januari 2021

C.9 NOS, 'Lek in GGD-systeem al driekwart jaar aanwezig', www.nos.nl, 28 januari 2021

C.10 RTL, 'GGD-voorzitter betuigt spijt, 'Systemen gaven ruimte voor datalek', www.rtl.nl, 29 januari 2021

C.11 NOS, 'Waakhond stelt GGD onder 'verscherpt toezicht', problemen al maanden bekend', www.nos.nl, 28 januari 2021

C.12 BNNVARA, 'Fraudehelpdesk, Gelekte GGD-gegevens vorig jaar al misbruikt', www.bnnvara.nl, 29 januari 2021

C.13 Parool, De Jonge in debat over GGD-datalek we hebben er onvoldoende aandacht voor gehad www.parool.nl, 3 februari 2021

C.14 Politie, 'In totaal nu 7 mensen aangehouden voor GGD-datadiefstal', www.politie.nl, 25 februari 2021

C.15 Autoriteit Persoonsgegevens, 'Boete Booking.com voor te laat melden datalek', www.autoriteitpersoonsgegevens.nl, 31 maart 2021

C.16 Consumentenbond, 'Datalekken, de gevaren en wat moet je doen?', www.consumentenbond.nl, 9 juni 2021

C.17 RTL, 'Datadiefstal GGD veel groter dan gemeld, gedupeerden niet geïnformeerd' www.rtl.nl, 12 augustus 2021

C.18 Nu, 'Criminelen gebruikten datalek bij callcenter om ouderen op te lichten', www.nu.nl, 22 oktober 2021

C.19 Autoriteit Persoonsgegevens, 'GGD moet persoonsgegevens beter beveiligen', www.autoriteitpersoonsgegevens.nl, 9 november 2021

C.20 Autoriteit Persoonsgegevens, 'AP beboet Transavia om slechte beveiliging persoonsgegevens', www.autoriteitpersoonsgegevens.nl, 12 november 2021

C.21 VPNGids, 'Wat is identiteitsfraude en hoe voorkom je het?', www.vpngids.nl, 25 november 2021

C.22 OM, 'Celstraf geeist voor diefstal en verkoop van gegevens GGD', www.om.nl, 14 januari 2022

C.23 Een Vandaag, 'Oud-Kamerlid PvdA pleit voor minister voor ICT, 'Als we GGD-datalek vergeten zijn, ligt er weer iets anders op straat', www.eenvandaag.avrotros.nl, 3 februari 2022

C.24 Nu, 'GGD heeft zaken op gebied van privacy nog altijd niet goed geregeld', www.nu.nl, 4 februari 2022

C.25 BNR, 'Geen oplossing datalek GGD? Dan massaclaim voor Kuipers', www.bnr.nl, 9 februari 2022

C.26 CBS, '2,5 miljoen Nederlanders in 2021 slachtoffer van online criminaliteit', www.cbs.nl, 1 maart 2022

C.27 Vrij Nederland, 'Astrid Oosenbrug, 'Iets positiefs halen uit negatieve ervaringen, dat kan ik wel', www.vn.nl, 2 maart 2022

C.28 Veilig Internetten, 'Wat is phishing?', www.veiliginternetten.nl

C.29 Politie, 'Wat is hacking?', www.vraaghetdepolitie.nl

C.30 Autoriteit Persoonsgegevens, 'Gerrit (72) werd slachtoffer van een datalek én een auto-inbraak. Toeval?', www.autoriteitpersoonsgegevens.nl

C.31 NOS, 'De privacywet wordt amper gehandhaafd, is meer geld de oplossing', www.nos.nl, 25 maart 2021

C.32 Politico, 'We have a huge problem' European regulator despairs over lack of enforcement. www.politico.eu 27 december 2019

C.33 Aantal privacyklachten blijft zorgwekkend hoog – www.autoriteitpersoonsgegevens.nl, 12 maart 2021

C.34 Forse stijging privacyklachten in 2019 - autoriteitpersoonsgegevens.nl, 14 februari 2020

C.35 Privacyautoriteit kan drukte niet aan, grove privacyschendingen dreigen. www.rtlnieuws.nl, 14 februari 2020

C.36 VPNGids.nl, AP 'Er zijn tienduizend wachtenden voor u', www.vpngids.nl

Categorie D Kamerstukken

D.1A *Handelingen II* 2020/21, nr. 52, item 3 (*Privacylek in de systemen van de GGD, gecorrigeerd stenogram*), 3 februari 2021 (eerste deel)

D.1B *Handelingen II* 2020/21, nr. 52, item 6 (*Privacylek in de systemen van de GGD, gecorrigeerd stenogram*), 3 februari 2021 (tweede deel)

D.2 *Kamerstukken II* 2020/21, 27 529, nr. 234 (*Verslag van een schriftelijk overleg*)

D.3 *Kamerstukken II* 2020/21, 27 529, nr. 235 (*Kamerbrief*)

D.4 Verschillende notulen Overleg SG LCT 5, bijlage 968379 bij *Kamerstukken II* 2020-2021, 27 529, nr. 236

D.5 *Kamerstukken II* , 2020-2021, 25 295, nr. 843

D.6 Feitenrelaas inzake gebeurtenissen omtrent coronatest-IT-systeem van de GGD, bijlage bij *Kamerstukken II* 2020-2021, 27 529, nr. 236.

D.7 Ministerie van Volksgezondheid, Welzijn en Sport, 'Kamerbrief over stand van zaken digitale ondersteuning pandemiebestrijding,' 12 februari 2021

D.8 *Kamerstukken II* 2020/21, 25 295, nr. 1105

D.9 *Kamerstukken II* 2020/21, 25 295, nr. 1179

D.10 *Kamerstukken II* 2020/21, 27 529, nrs. 244, 245, 246, 250, 251

D.11 *Kamerstukken II* 2020/21, 2021D33012

D.12 *Kamerstukken I* 20222/23, 36 034, nr. B (*MvA*)

Categorie E Literatuur, deskundigenrapporten en normen

E.1 European Union Agency for Fundamental Rights, 'Access to Data Protection Remedies in EU Member States. Accessing remedies in the area of data protection, experiences of individuals', Luxemburg: Publications Office of the European Union 2013

E.2 H. Koch, S. Midgley & E. Riggs, 'Psychological Injury, Cyber Crime and Data Breach Damages', *The Expert Witness*, 18 april 2019

E.3 J. Guyn, ‘Anxiety, depression and PTSD, The hidden epidemic of data breaches and cybercrimes’, *USA Today*

E.4 I. Kilovaty, ‘Psychological Data Breach Harms’, *North Carolina Journal of Law & Technology*, 23-1 (2021)

E.5 Aleid Wolfsen, ‘Smartengeld’, www.autoriteitpersoonsgegevens.nl, 22 februari 2021

Categorie F Communicatie vanuit GGD GHOR

F.1 Over GGD GHOR

F.2 Benchmark GGD'en

F.3 GGD GHOR GGD en haar data - Hoe zit het echt? Een repliek d.d. 29 januari 2021

F.4 GGD GHOR informatie over verwijderen informatie d.d. 12 februari 2021

F.5 Veelgestelde vragen over de datadiefstal op www.ggdghor.nl (update 28 januari 2021)

F.6 Veelgestelde vragen over de datadiefstal op www.ggdghor.nl (update 29 januari 2021)

F.7 Veelgestelde vragen over de datadiefstal op www.ggdghor.nl (update 30 januari 2021)

F.8 Veelgestelde vragen over de datadiefstal op www.ggdghor.nl (update 3 februari 2021)

F.9 Veelgestelde vragen over de datadiefstal op www.ggdghor.nl (update 25 februari 2021)

F.10 Veelgestelde vragen over de datadiefstal op www.ggdghor.nl (update 19 maart 2021)

F.11 Veelgestelde vragen over de datadiefstal op www.ggdghor.nl (update 20 april 2021)

F.12 Veelgestelde vragen over de datadiefstal op www.ggdghor.nl (update 28 februari 2022)

F.13 Veelgestelde vragen over de datadiefstal op www.ggdghor.nl (update 5 april 2022)

F.14 Veelgestelde vragen over de datadiefstal op www.ggdghor.nl (update 14 juli 2021)

F.15 Veelgestelde vragen over de datadiefstal op www.ggdghor.nl (update 30 september 2022)

F.16 Screenshot website GGD GHOR, 'Privacyverklaring testen op het coronavirus' (8 maart 2022)

F.17 Screenshot website GGD GHOR, 'Privacyverklaring vaccinatie tegen het coronavirus' (8 maart 2022)

F.18 Privacyverklaring landelijke capaciteit bron- en contactonderzoek COVID-19 (april 2021)

F.19 Screenshot website GGD GHOR, 'Politieonderzoek naar verdachten datadiefstal afgerond' (5 april 2022)

F.20 Brief van GGD GHOR aan een Gedupeerde d.d. 16 april 2021 (excuusbrief) (geanonimiseerd)

F.21 Brief van GGD GHOR aan een gedupeerde d.d. 25 april 2022 (financieel gebaar) (geanonimiseerd)

Categorie G Woo-stukken

G.1 GGD GHOR, Landelijke referentie DPIA CoronIT voor GGD’en

G.2 Beveiligingsrisico bevindingen en maatregelen GGD Corona applicaties Groei-voortgangsdocument, Versie d.d. 25 juni 2021, GGD Haaglanden

G.3 Landelijke werkinstructie Bron- en Contactonderzoek, Versie 14062021

G.4 Memo advies opstellen autorisatiematrices HPZone en HPZone Lite d.d. 30 april 2021, GGD Haaglanden

G.5 Advies intrekken admin accounts HPZone medewerkers, d.d. 8 maart 2021, GGD Haaglanden

G.6 Brief GGD GHOR d.d. 27 juli 2021

G.7 GGD GHOR, Overzicht getroffen maatregelen HPZone en CoronIT d.d. 29 januari 2021

G.8 Activiteiten ten aanzien van autorisaties, GGD Haaglanden

G.9 Plan van aanpak Project “naar veilige GGD-Corona systemen” d.d. 3 februari 2021, GGD Haaglanden

G.10 Wijzigingsvoorstel G, Schijf map CORONA d.d. 10 januari 2021, GGD Haaglanden

G.11 Data Protection Impact Assessment HP Zone en HP Zone Lite d.d. 26 april 2021, GGD regio Utrecht

G.12 Mail Opschonen gebruikers Webhelp in HPZone d.d. 19 februari 2021, GGD Drenthe

G.13 GGD GHOR procesvoorstel autorisatiemanagement landelijke medewerkers HPZone Lite d.d. 25 februari 2021

G.14 Mailwisseling rollen rechten autorisaties HPZone d.d. 8 februari 2021, GGD Drenthe

G.15 GGD GHOR, DPIA Nationale Capaciteit Bron- & Contactonderzoek november 2020

G.16 GGD GHOR, Concept Landelijke referentie DPIA voor GGD'en (vaccinaties)

G.17 GGD GHOR, Concept procesvoorstel autorisatiemanagement HPZone Lite d.d. 10 februari 2021

G.18 Herzien opschalingsplan testen en bron- en contactonderzoek najaar 2020, GGD Flevoland

G.19 Notulen overleg Data GGD Covid-19 d.d. 9 februari 2021, GGD Flevoland

G.20 Beleid en procesbeschrijving voor toegangsbeveiliging d.d. 17 februari 2021, GGD Gelderland-Zuid

G.21 Bijlage bij oplegnotitie DPG BCO bestanden BYOD BYOT d.d. 22 juni 2021

G.22 Beleid Logische Toegangsbeveiliging d.d. 16 november 2021, GGD IJsselland

G.23 Protocol Toegangs- en autorisatiebeheer Applicaties Coronaketen d.d. 29 september 21, GGD IJsselland

G.24 GGD GHOR,”Rollen en rechten in CoronIT in relatie tot toegang tot persoonsgegevens d.d. 18 mei 2020

G.25 E-mailwisseling inzake privacy rond CoronIT d.d. 25 mei 2020, GGD Rotterdam-Rijnmond

G.26 E-mailwisseling inzake Proces van handeling nav inzage dossier d.d. 6 november 2020, GGD Rotterdam-Rijnmond

G.27 Memo advies DPIA corona app voor bron- en contactonderzoek d.d. 6 januari 2021, GGD Rotterdam-Rijnmond

G.28 Conceptverslag Bestuurlijke adviescommissie Publieke Gezondheid d.d. 5 februari 2020

G.29 Programmateam Corona GGD-GHOR (Concept)verslag vergaderdatum 30 november en 2 december 2021, GGD Rotterdam-Rijnmond

G.30 Mail inzake convenant gegevensuitwisseling gezamenlijk verantwoordelijken d.d. 19 januari, GGD Rotterdam-Rijnmond

G.31 Overeenkomst gebruik notificatieapplicatie Ministerie VWS-GGD'en d.d. 26 augustus 2020, GGD Rotterdam-Rijnmond

G.32 Mail inzake DPIA's deel 1 d.d. 19 januari 2021, GGD Rotterdam-Rijnmond

G.33 Data Protection Impact Assessment (DPIA) GGD Contact ter ondersteuning BCO d.d. 12 april 2021, GGD Rotterdam-Rijnmond

G.34 Mail inzake Agenda en stukken vergadering BacPG d.d. 5 februari 2021, GGD Rotterdam-Rijnmond

G.35 Oplegnotitie DPIA Testen Programmateam Corona GGD-GHOR d.d. 17 juli 2020, GGD Rotterdam-Rijnmond

G.36 Oplegnotitie DPIA BCO Programmateam Corona GGD-GHOR d.d. 15 juli 2021, GGD Rotterdam-Rijnmond

G.37 Oplegnotitie VOG medewerkers Programmateam Corona GGD-GHOR d.d. 9 februari 2021, GGD Rotterdam-Rijnmond

G.38 Oplegnotitie voortgang DPIA's en privacyprogramma Corona-organisatie d.d. 7 oktober 2021, GGD Rotterdam-Rijnmond

G.39 Notitie uitfasering HPzone Lite Programmateam Corona GGD-GHOR d.d. 2 februari 2021, GGD Rotterdam-Rijnmond

G.40 Mail Terugkoppeling/MT Corona 26 januari, agenda en stukken d.d. 27 januari 2021, GGD Rotterdam-Rijnmond

G.41 Mail inzake Besluitvorming HP Zone d.d. 1 februari 2021, GGD Rotterdam-Rijnmond

G.42 Memo MT inzake Consequenties brief GGD GHOR, Update en noodzakelijke acties betreffende queries HPZone en HPZone Lite d.d. 5 februari 2021

G.43 Brief aan de Ondernemingsraad van GGD Noord- en Oost-Gelderland inzake Instemming monitoring logging covidsystemen d.d. 23 juli 2021, GGD Noord- en Oost-Gelderland

G.44 Mail inzake Update data-diefstal d.d. 28 januari 2021, GGD Noord- en Oost-Gelderland

G.45 Actieplan Informatiebeveiliging, GGD Noord- en Oost-Gelderland

G.46 Projectplan Awarenesscampagne Informatiebeveiliging 2021 d.d. 15 februari 2021, GGD Noord- en Oost-Gelderland

G.47 Brief Dirkzwager aan GGD Noord- en Oost-Gelderland inzake GGD NOG / verantwoordelijkheden gegevensuitwisselingen GGD d.d. 15 maart 2021

G.48 Brief Dirkzwager aan GGD Noord- en Oost-Gelderland inzake GGD NOG / verantwoordelijkheden gegevensuitwisselingen GGD d.d. 26 maart 2021

G.49 Adviesnota dagelijks bestuur inzake Ontwikkelingen datadiefstal COVID-19-systemen d.d. 15 februari 2021, GGD Noord- en Oost-Gelderland

G.50 Brief aan het algemeen bestuur van GGD Noord- en Oost-Gelderland en Veiligheidsregio Noord- en Oost-Gelderland inzake datadiefstal covid-systemen d.d. 29 januari 2021

G.51 Agenda Projectgroep COVID19 d.d. 1 februari 2021, GGD Noord- en Oost-Gelderland

G.52 Verslag voortgangsoverleg periode 05 d.d. 20 april 2021, GGD Haaglanden

G.53 Convenant gegevensuitwisseling inzake nationale capaciteit bron- en contactonderzoek

G.54 Mailwisseling inzake GGD en Governance d.d. 28 augustus 2020, GGD Rotterdam-Rijnmond

G.55 Rapport Utilis inzake Onderzoek technische kwaliteit en continuïteit HPZone Lite d.d. 5 februari 2021

G.56 KPMG rapportage QA Testen en Vaccinatie IT Quick-Scan vervanging HPZone d.d. 12 februari 2021

G.57 KPMG Rapportage IT Assessment GGD GHOR d.d. 5 januari 2021

G.58 Axis into ICT Analyse database HPZone Januari-februari 2021

G.59 Weekverhaal, week 24. Programma Corona GGD-GHOR d.d. 14 juni 2021

Categorie H Correspondentie met de Gedaagden

H.1 Correspondentie met de Staat

H.1A Brief van de advocaten van Stichting ICAM aan de Staat der Nederlanden d.d. 8 februari 2022

H.1B Brief van de Staat der Nederlanden aan de advocaten van Stichting ICAM d.d. 1 maart 2022

H.1C Brief van de advocaten van Stichting ICAM aan de Staat der Nederlanden d.d. 9 maart 2022

H.1D Brief van Stichting ICAM aan de Staat der Nederlanden d.d. 4 mei 2022

H.1E Brief van de advocaten van de Staat der Nederlanden aan de advocaten van Stichting ICAM d.d. 24 mei 2022

H.1F Brief van de advocaten van Stichting ICAM aan de advocaten van de Staat der Nederlanden d.d. 28 juli 2022

H.2 Correspondentie met GGD GHOR

H.2A Brief van de advocaten van Stichting ICAM aan Stichting Verenigingsbureau Publieke Gezondheid en Veiligheid Nederland d.d. 8 februari 2022

H.2B Brief van de advocaten van Stichting ICAM aan Vereniging Publieke Gezondheid en Veiligheid Nederland d.d. 8 februari 2022

H.2C Brief van de advocaten van Stichting ICAM aan Stichting Projectenbureau Publieke Gezondheid en Veiligheid Nederland d.d. 8 februari 2022

H.2D Bijlagen zoals bij de brieven in producties H.2A, H.2B en H.2C

H.2E Brief van GGD GHOR aan de advocaten van Stichting ICAM d.d. 1 maart 2022

H.2F Brief van de advocaten van Stichting ICAM aan GGD GHOR d.d. 10 maart 2022

H.2G Brief van GGD GHOR aan de advocaten van Stichting ICAM d.d. 16 maart 2022

H.2H Brief van de advocaten van Stichting ICAM aan de advocaten van GGD GHOR d.d. 13 april 2022

H.2I Brief van Stichting ICAM aan GGD GHOR d.d. 4 mei 2022

H.2J Brief van de advocaten van GGD GHOR aan de advocaten van Stichting ICAM d.d. 13 mei 2022

H.2K Brief van de advocaten van GGD GHOR aan de advocaten van Stichting ICAM d.d. 25 mei 2022

H.2L Brief van de advocaten van Stichting ICAM aan de advocaten van GGD GHOR d.d. 8 juli 2022

H.2M Brief van de advocaten van GGD GHOR aan de advocaten van Stichting ICAM d.d. 21 juli 2022

H.2N Brief van de advocaten van Stichting ICAM aan de Stichting Landelijke Coördinatie COVID-19 Bestrijding d.d. 22 november 2022

H.2O Brief van de Stichting Landelijke Coördinatie COVID-19 Bestrijding aan de advocaten van Stichting ICAM d.d. 10 januari 2023

H.3 Correspondentie met de Gemeenten

H.3A Brieven van de advocaten van Stichting ICAM aan de Gemeente Rotterdam en aan de Gemeente Amsterdam d.d. 8 februari 2022

H.3B Bijlagen zoals bij de brieven in productie H.3A

H.3C Brief van de Gemeente Rotterdam aan de advocaten van Stichting ICAM d.d. 18 maart 2022 en van de Gemeente Amsterdam aan de advocaten van Stichting ICAM d.d. 28 maart 2022

H.4 Correspondentie met de GGD'en

H.4A Brieven van de advocaten van Stichting ICAM aan alle 25 GGD'en d.d. 8 februari 2022

H.4B Bijlagen zoals bij de brieven in productie H.4A

H.5 Correspondentie met de Veiligheidsregio's

H.5A Brieven van de advocaten van Stichting ICAM aan de Veiligheidsregio Rotterdam-Rijnmond en aan de Veiligheidsregio Amsterdam-Amstelland d.d. 8 februari 2022

H.5B Bijlagen zoals bij alle brieven in productie H.5A

H.5C Brief van het Veiligheidsberaad aan de advocaten van Stichting ICAM d.d. 21 februari 2022

Categorie I Woo-correspondentie en Woo-dossiers

I.1 Correspondentie met het ministerie van VWS

I.1A Brief van de advocaten van Stichting ICAM aan het ministerie van VWS d.d. 15 februari 2022

I.1B Brief van het ministerie van VWS aan de advocaten van Stichting ICAM d.d. 18 maart 2022

I.1C E-mail van de advocaten van Stichting ICAM aan het ministerie van VWS d.d. 17 mei 2022

I.1D E-mail van het ministerie van VWS aan de advocaten van Stichting ICAM d.d. 7 juni 2022

I.1E Brief van de advocaten van Stichting ICAM aan het ministerie van VWS d.d. 28 juli 2022

I.1F Brief van het ministerie van VWS aan de advocaten van Stichting ICAM d.d. 29 juli 2022

I.2 Correspondentie met GGD GHOR

I.2A Brieven van de advocaten van Stichting ICAM aan GGD GHOR d.d. 15 februari 2022

I.2B Brieven van GGD GHOR aan de advocaten van Stichting ICAM d.d. 1 april 2022

I.2C Brieven van de advocaten van Stichting ICAM aan GGD GHOR d.d. 16 mei 2022

I.2D Brieven van GGD GHOR aan de advocaten van Stichting ICAM d.d. 19 mei 2022

I.2E Brief van de advocaten van Stichting ICAM GGD aan de advocaten van GHOR d.d. 8 juli 2022

I.2F Brieven van GGD GHOR aan de advocaten van Stichting ICAM d.d. 22 juli 2022

I.3 Correspondentie met de Gemeenten

I.3A Brief van de advocaten van Stichting ICAM aan de Gemeente Amsterdam d.d. 15 februari 2022

I.4 Correspondentie met de Veiligheidsregio's

I.4A Brief van de advocaten van Stichting ICAM aan de Veiligheidsregio Amsterdam-Amstelland d.d. 15 februari 2022

I.5 Correspondentie AP

I.5A Brief van de advocaten van Stichting ICAM aan de Autoriteit Persoonsgegevens 8 juni 2022

I.5B E-mailcorrespondentie tussen de advocaten van Stichting ICAM en de Autoriteit Persoonsgegevens d.d. 20 juni 2022 t/m 19 januari 2023

I.5C E-mail van de Autoriteit Persoonsgegevens aan de advocaten van Stichting ICAM d.d. 26 juli 2022

I.6 Woo-dossier Stichting ICAM/GGD Amsterdam

I.7 Woo-dossier Stichting ICAM/GGD Drenthe

I.8 Woo-dossier Stichting ICAM/GGD Rotterdam-Rijnmond

I.9 Woo-dossier Stichting ICAM/GGD Zeeland

Categorie J Strafvonnissen

J.1 Rechtbank Midden-Nederland 28 januari 2022, parketnummer 16/041344-21

J.2 Rechtbank Midden-Nederland 12 januari 2022, ECLI:NL:RBMNE:2022:55

J.3 Rechtbank Midden Nederland 14 september 2021, ECLI:NL:RBMNE:2021:4419

J.4 Rechtbank Midden-Nederland 14 september 2021, ECLI:NL:RBMNE:2021:4434

J.5 Rechtbank Midden-Nederland 28 januari 2022, parketnummer 16/041344-21

Categorie K Overig

K.1 Eindbrief onderzoek beveiliging persoonsgegevens GGD GHOR en GGD'en van de Autoriteit Persoonsgegevens d.d. 8 november 2021

K.2 KPMG, 'Whitepaper privacyonderzoek 2021, Meer zorgen over privacy. Het resultaat van ons privacy onderzoek onder consumenten', KPMG: oktober 2021

K.3 Screenshot Website Rijksoverheid 'Veiligheidsregio's', www.rijksoverheid.nl

K.4 Screenshot Website Rijksoverheid 'Taken van een gemeente', www.rijksoverheid.nl

K.5 Dienstverleningsovereenkomst ARVODI-2018, Opdracht aan GGD-GHOR voor het ontwikkelen en implementeren van CoronlT, november 2020

K.6 Dienstverleningsovereenkomst ARVODI-2018, Opdracht aan GGD-GHOR voor het doen oprichten van een klantcontactcentrum, juni 2020

K.7 E-mail [gedupeerde 1] aan Stichting ICAM d.d. 6 december 2021

K.8 E-mail [gedupeerde 2] aan Stichting ICAM d.d. 7 december 2021

K.9 E-mail [gedupeerde 3] aan Stichting ICAM d.d. 8 december 2021

K.10 E-mail [gedupeerde 4] aan Stichting ICAM d.d. 15 december 2021

K.11 E-mail [gedupeerde 5] aan Stichting ICAM d.d. 28 december 2021

K.12 E-mail [gedupeerde 6] aan Stichting ICAM d.d. 11 december 2021

K.13 E-mail [gedupeerde 7] aan Stichting ICAM d.d. 7 december 2021

K.14 E-mail [gedupeerde 8] aan Stichting ICAM d.d. 6 december 2021

K.15 E-mail [gedupeerde 9] aan Stichting ICAM d.d. 7 december 2021

K.16 E-mail [gedupeerde 10] aan Stichting ICAM d.d. 6 december 2021

K.17 E-mail [gedupeerde 11] aan Stichting ICAM d.d. 8 december 2021

K.18 E-mail [gedupeerde 12] aan Stichting ICAM d.d. 15 december 2021

K.19 E-mail [gedupeerde 13] aan Stichting ICAM d.d. 23 december 2021

K.20 E-mail [gedupeerde 14] aan Stichting ICAM d.d. 24 februari 2022

K.21 Screenshot Website Autoriteit Persoonsgegevens, 'Zorgverleners en de AVG', www.autoriteitpersoonsgegevens.nl, 31 mei 2022.

K.22 Verslagen Begeleidingscommissie Digitale Ondersteuning Bestrijding COVID-19

K.23 Anonieme brief

K.24 Nederlands Instituut Publieke Veiligheid, ‘De rol van het Veiligheidsberaad tijdens de coronacrisis’

K.25 Dienstverleningsovereenkomst ARVODI-2018, Opdracht aan GGD-GHOR voor het realiseren van digitale randvoorwaarden ten behoeve van de bestrijding van COVID-19

K.26 Brief van de Autoriteit Persoonsgegevens (Afronding onderzoek beveiliging GGD corona) d.d. 29 september 2022