Geschillenkamer

Beslissing ten gronde 166/2024 van 17 december 2024

In zijn arrest 2025/AR/74 van 3 september 2025 heeft het Hof van Beroep deze beslissing gedeeltelijk vernietigd en heeft het, **gebruikmakend van haar volle rechtsmacht**, de door de Geschillenkamer opgelegde administratieve boete verlaagd tot 50.000 euro.

De GBA heeft een cassatievoorziening ingesteld tegen het arrest 2025/AR/74 van het Marktenhof van 3 september 2025, waarbij deze beslissing werd vernietigd..

Dossiernummer: DOS-2021-06114

Betreft: door een ziekenhuis getroffen beveiligingsmaatregelen

De Geschillenkamer van de Gegevensbeschermingsautoriteit (hierna "GBA"), samengesteld uit de heer Hielke HIJMANS, voorzitter, en de heren Romain Robert en Jelle Stassijns, leden;

Gelet op Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), hierna "AVG";

Gelet op de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit[1], hierna "WOG";

Gelet op het Reglement van interne orde (hierna "RIO")[2], zoals goedgekeurd door de Kamer van volksvertegenwoordigers op 20 december 2018 en gepubliceerd in het Belgisch Staatsblad op 15 januari 2019;

Gelet op de stukken van het dossier;

Heeft de volgende beslissing genomen inzake:

De verweerder: Y, vertegenwoordigd door meester Victoria Ruelle en meester Fanny Cotton, hierna "de verweerder".

---

[1] De GBA herinnert eraan dat de herziene kaderwet op 1 juni 2024 in werking is getreden. Zij is alleen van toepassing op klachten, bemiddelingsdossiers, verzoeken, inspecties en procedures voor de Geschillenkamer die vanaf die datum zijn aangevangen. Dossiers die zijn aangevat vóór 1 juni 2024, zoals het onderhavige dossier, zijn onderworpen aan de bepalingen van de oude versie van de WOG, die hier kan worden geraadpleegd: https://www.gegevensbeschermingsautoriteit.be/publications/organieke-wet-van-de-gba.pdf.

[2] De GBA herinnert eraan dat het nieuwe Reglement van interne orde op 1 juni 2024 in werking is getreden. Het is alleen van toepassing op klachten, bemiddelingsdossiers, verzoeken, inspecties en procedures voor de Geschillenkamer die vanaf die datum zijn aangevangen. Dossiers die zijn aangevat vóór 1 juni 2024, zoals het onderhavige dossier, zijn onderworpen aan de bepalingen van de oude versie van het RIO, die hier kan worden geraadpleegd: https://www.gegevensbeschermingsautoriteit.be/publications/reglement-van-interne-orde.pdf.

I. Feiten en procedure

1. De verweerder is een ziekenhuisinstelling gevestigd in België. Op [datum] 2021 stelt de verweerder de GBA in kennis van een gegevensinbreuk waarbij losgeld werd geëist ("ransomware"). Deze inbreuk heeft plaatsgevonden tussen 16 en [datum] 2021. Op [datum] 2021 dient de verweerder een aanvullende melding in met betrekking tot deze gegevensinbreuk.

2. Op 20 oktober 2021 schakelt het Directiecomité de Inspectiedienst in krachtens artikel 63, 1°, van de WOG, nadat het heeft vastgesteld dat er ernstige aanwijzingen zijn voor het bestaan van een praktijk die aanleiding kan geven tot een inbreuk op de grondbeginselen van de bescherming van persoonsgegevens.

3. Op 22 november 2021 richt de Inspectiedienst, in het kader van een inspectieonderzoek naar de gegevensinbreuk, een verzoek om informatie aan de verweerder. Op 22 december 2021 dient de verweerder zijn antwoorden op dit verzoek om informatie in.

4. Op 11 februari 2022 verzoekt de Inspectiedienst om aanvullende informatie in het kader van dit inspectieonderzoek, met name om de door de verweerder getroffen technische en organisatorische maatregelen beter te kunnen beoordelen. Op 10 maart 2022 verstrekt de verweerder zijn antwoorden op dit verzoek om aanvullende informatie.

5. Op 28 april 2022 stelt de Inspectiedienst een technologisch onderzoeksverslag op. Op 20 juni 2022 sluit de Inspectiedienst het onderzoek af en maakt hij het dossier over aan de voorzitter van de Geschillenkamer overeenkomstig artikel 91, § 1 en § 2, van de WOG.

6. Het verslag bevat vaststellingen over de gegevensinbreuk. De Inspectiedienst concludeert in het bijzonder dat, hoewel de gegevensinbreuk ontegensprekelijk het gevolg is van de externe inbraak in de infrastructuur van de verweerder, de omvang ervan onzeker blijft.

7. Het onderzoeksverslag bevat ook vaststellingen met betrekking tot het ontbreken van een gegevensbeschermingseffectbeoordeling en de ontoereikendheid van de technische en organisatorische maatregelen die door de verweerder zijn getroffen. De Inspectiedienst stelt in grote lijnen het volgende vast:

   a. **Vaststelling 1**: inbreuk op artikel **35.3** van de AVG wegens het ontbreken van een gegevensbeschermingseffectbeoordeling (hierna "GEB");

   b. **Vaststelling 2**: inbreuk op de artikelen **5.1.f) en 32** van de AVG wegens het ontbreken van een effectief en formeel beleid voor informatieveiligheid op het moment van de gegevensinbreuk;

c. **Vaststelling 3**: inbreuk op de artikelen **5.1.f), 24 en 32** van de AVG wegens de ondoeltreffendheid van het beleid en/of de procedure voor het bijwerken van de beveiliging van IT-apparatuur (software);

d. **Vaststelling 4**: inbreuk op de artikelen **5.1.f), 24 en 32** van de AVG vanwege andere ontbrekende beveiligingsmaatregelen, namelijk:

i. het ontbreken van een echt opleidings-/bewustmakingsprogramma voor werknemers;

ii. het ontbreken van een systeem voor het bewaren van logbestanden met het oog op latere analyses bij incidenten;

iii. het ontbreken van systematische audits van de kwaliteit van de beveiliging van persoonsgegevens; en

iv. de zwakke beveiliging van het wachtwoord voor toegang tot het elektronische patiëntendossier.

8. Op 27 september 2022 beslist de Geschillenkamer op grond van artikel 95, § 1, 1°, en artikel 98 van de WOG dat het dossier gereed is voor behandeling ten gronde. Op dezelfde dag wordt de verweerder per aangetekende zending in kennis gesteld van de bepalingen zoals vermeld in artikel 95, § 2, en in artikel 98 van de WOG. Tevens wordt hij op grond van artikel 99 van de WOG op de hoogte gebracht van de termijn voor het indienen van zijn conclusie. De uiterste datum voor ontvangst van de conclusie van antwoord van de verweerder werd vastgelegd op 8 november 2022. De verweerder heeft een verzoek tot verlenging van de termijn voor het indienen van de conclusie ingediend, dat op 14 oktober 2022 is ingewilligd.

9. Op 8 oktober 2022 vraagt de verweerder per e-mail om een kopie van het dossier (artikel 95, § 2, 3°, van de WOG), die hem op 14 oktober 2022 elektronisch wordt bezorgd.

10. Op 22 november 2022 ontvangt de Geschillenkamer de conclusie van antwoord van de verweerder. Samengevat voert de verweerder de volgende verweermiddelen aan:

- **Over de procedure**:

a. De onregelmatigheid van de inschakeling van het Directiecomité door het Algemeen Secretariaat.

b. De ongeldigheid van het proces-verbaal van het Directiecomité.

c. De onjuistheid van de ernstige aanwijzingen die door het Directiecomité in aanmerking zijn genomen.

d. De onmogelijkheid om het meldingsformulier binnen de afdelingen van de GBA door te geven.

- **Over de inhoud**:

  a. **Vaststelling 1**: de verweerder stelt dat er een effectbeoordeling is uitgevoerd.

  b. **Vaststelling 2**: de verweerder stelt dat het beleid voor informatieveiligheid van het ziekenhuis moet worden gezien als een onderdeel van een reeks documenten en procedures die zijn ingesteld en die de organisatorische en technische maatregelen van het ziekenhuis vormen.

  c. **Vaststelling 3**: de verweerder stelt dat het beleid voor het bijwerken van de beveiliging van IT-apparatuur bestaat uit consultancycontracten die het ziekenhuis heeft gesloten om een maandelijkse controle van zijn installaties te waarborgen, en betrekking heeft op verschillende maatregelen die het ziekenhuis na de gegevensinbreuk heeft getroffen.

  d. **Vaststelling 4**: de verweerder stelt dat alle maatregelen die zouden ontbreken, zijn ingevoerd.

11. In zijn conclusie geeft de verweerder te kennen dat hij voornemens is gebruik te maken van de mogelijkheid om te worden gehoord, overeenkomstig artikel 98 van de WOG.

12. Op 20 juni 2024 worden de partijen ervan in kennis gesteld dat de hoorzitting op 4 juli 2024 zal plaatsvinden.

13. Op 4 juli 2024 worden de partijen gehoord door de Geschillenkamer.

14. Op 22 juli 2024 wordt het proces-verbaal van de hoorzitting aan de partijen voorgelegd.

15. Op 29 juli 2024 ontvangt de Geschillenkamer de opmerkingen van de verweerder over het proces-verbaal.

16. Op 13 augustus 2024 deelt de Geschillenkamer de verweerder haar voornemen mee om een administratieve geldboete op te leggen, evenals het bedrag daarvan, teneinde de verweerder in de gelegenheid te stellen zijn argumenten ter zake naar voren te brengen.

17. Op 3 september 2024 ontvangt de Geschillenkamer de reactie van de verweerder op het voornemen om een administratieve geldboete op te leggen en op het bedrag ervan. De verweerder voert aan dat het ziekenhuis moet worden beschouwd als een "overheid" in de zin van artikel 5[3] van de wet van 30 juli 2018 betreffende de

[3] Artikel 5 van de kaderwet bepaalt het volgende: "Voor de toepassing van deze wet wordt verstaan onder "overheid" :
1° de Federale Staat, de deelstaten en lokale overheden;
2° de rechtspersonen van publiek recht die van de Federale Staat, de deelstaten of lokale overheden afhangen;

bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (hierna "kaderwet"), zodat het niet mogelijk is om hem een geldboete op te leggen[4]. Bovendien betwist het ziekenhuis, indien het als een rechtspersoon zou worden beschouwd waaraan een geldboete kan worden opgelegd, zowel het principe van het opleggen van een geldboete als het bedrag ervan, zoals vastgesteld door de Geschillenkamer in het sanctieformulier. Hij voert argumenten aan met betrekking tot de geringe ernst van de inbreuk en de beperkte financiële draagkracht van het ziekenhuis.

II. Motivering

II.1. Achtergrond[5]

18. Op [datum] 2021 heeft de verweerder een gegevensinbreuk van het type "ransomware" gemeld aan de GBA, die zich had voorgedaan tussen [...] en [datum] 2021. Op [datum] 2021 heeft de verweerder een aanvullende melding over deze gegevensinbreuk ingediend.

19. Op [datum] 2021 heeft de verweerder ook een persbericht gepubliceerd om het publiek te informeren dat een cyberaanval had plaatsgevonden. Daarin lichtte hij toe dat zijn servers waren getroffen, wat leidde tot een verstoring van een deel van het computersysteem.

20. Uit zowel de initiële als de aanvullende melding van de gegevensinbreuk blijkt dat tal van categorieën van persoonsgegevens in het gedrang waren gebracht, waaronder bijzondere categorieën van persoonsgegevens (zoals gezondheidsgegevens) en gegevens uit elektronische communicatie. Bovendien bevestigde de aanvullende melding dat het maximale aantal betrokkenen bij de inbreuk 300.000 bedroeg, en dat het risiconiveau voor de rechten en vrijheden van de betrokkenen als "hoog" was ingeschat.

3° de personen, ongeacht hun vorm en aard, die :

- opgericht zijn met het specifieke doel te voorzien in behoeften van algemeen belang die niet van industriële of commerciële aard zijn; en

- rechtspersoonlijkheid hebben; en

- waarvan hetzij de activiteiten in hoofdzaak door de overheden of instellingen vermeld in de bepalingen onder 1° of 2°, worden gefinancierd, hetzij het beheer onderworpen is aan toezicht door deze overheden of instellingen, hetzij de leden van het bestuursorgaan, leidinggevend orgaan of toezichthoudend orgaan voor meer dan de helft door deze overheden of instellingen zijn aangewezen;

4° de verenigingen bestaande uit één of meer overheden als bedoeld in de bepalingen onder 1°, 2° of 3°."

[4] Artikel 221, § 2, van de kaderwet bepaalt het volgende: "Het artikel 83 van de Verordening is niet van toepassing op de overheid en hun aangestelden of gemachtigden, tenzij het gaat om een publiekrechtelijke rechtspersoon die goederen of diensten aanbiedt op een markt."

[5] De feiten zoals ze in dit deel worden weergegeven, zijn gebaseerd op de conclusie van de verweerder en het verslag van de Inspectiedienst. Ze worden niet betwist door de verweerder.

21. Uit het onderzoek van de Inspectiedienst blijkt dat de inbraak werd gepleegd door een hacker vanaf servers op het Aziatische continent, via de e-mailserver Microsoft Exchange. De hacker had het antivirusprogramma verwijderd en vervolgens malware geïnstalleerd. Op die manier kon hij een account aanmaken met "beheerderstoegang".

22. De hacker had vervolgens BitLocker geactiveerd, waardoor alle toegang tot de gegevens op de Windows-servers van het ziekenhuis werd geblokkeerd. Wanneer iemand probeerde in te loggen, werd de toegang geweigerd en verscheen een losgeldeis. De hacker had bovendien de wachtwoorden van de Windows-computerservers gewijzigd om de toegang te verhinderen. Tijdens de aanval werd door de hacker ongeveer 5 gigabyte aan informatie geëxporteerd.

23. Tijdens de aanval werden de netwerkverbindingen naar buiten verbroken. Het ziekenhuisnoodplan (hierna "ZNP") werd geactiveerd om de continuïteit van de patiëntenzorg te waarborgen, met uitzondering van de spoedeisende hulp van het ziekenhuis, die gedurende 3 dagen gesloten was, maar waarvoor de maatregelen van het ZNP het mogelijk maakten om patiënten door te verwijzen naar andere spoedeisende hulpafdelingen van derde instellingen.

24. In zijn antwoorden op de vragen van de Inspectiedienst bevestigt het ziekenhuis dat op 20 september 2021 – 3 dagen na de gegevensinbreuk – de software die toegang geeft tot de patiëntendossiers voor 95 % operationeel was. Op [datum] 2021 – 12 dagen na de gegevensinbreuk – waren de e-maildiensten van het personeel opnieuw operationeel en beschouwde het ziekenhuis de gevolgen van de aanval grotendeels als verholpen.

25. Het gaat om de tweede gegevensinbreuk van het type "ransomware" die het ziekenhuis in tweeënhalf jaar tijd heeft ondergaan; de eerste vond plaats op [datum] 2019. Die eerste inbreuk werd rechtmatig aan de GBA gemeld.

II.2. Over de procedure

II.2.1. Inschakeling van het Directiecomité door het Algemeen Secretariaat:

26. **De verweerder** betoogt in zijn conclusie dat het Algemeen Secretariaat van de GBA niet bevoegd is om meldingen van gegevensinbreuken te behandelen op grond van de artikelen 19 en 20 van de WOG. Bijgevolg is de bevoegdheid van het Algemeen Secretariaat om meldingen van gegevensinbreuken te analyseren en vervolgens een nota op te stellen voor het Directiecomité niet vastgelegd. In ieder geval had deze nota overeenkomstig artikel 4 van het Reglement van interne orde ten minste een

week vóór de zitting van het Directiecomité moeten worden verzonden, maar de nota van het Algemeen Secretariaat is niet gedateerd.

27. **De Geschillenkamer** herinnert eraan dat artikel 4 van het RIO het volgende bepaalt: "Voor alle gevallen waar een beleidsbeslissing van het directiecomité noodzakelijk is, wordt door de bevoegde directeur een voorstel uitgewerkt aan de hand van een nota. Behalve in geval van dringende noodzakelijkheid zal het dossier minstens één week voor de zitting ter beschikking van de leden worden gesteld, desgevallend met inbegrip van de vereiste bijlagen. Ter zitting zal de bevoegde directeur het dossier toelichten."

28. De AVG bepaalt in artikel 33.1 dat "indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, [...] de verwerkingsverantwoordelijke deze (...) aan de (...) bevoegde toezichthoudende autoriteit [meldt] (...)", zonder onderscheid te maken tussen de bevoegde afdeling of dienst van de autoriteit om de inbreuk te behandelen. De Geschillenkamer merkt op dat noch de WOG, noch het RIO een afdeling van de GBA de exclusieve bevoegdheid toekent om meldingen van gegevensinbreuken te behandelen. In tegenstelling tot wat de verweerder tijdens de hoorzitting beweert, bestaat er op dit punt geen juridisch vacuüm, aangezien de AVG bepaalt dat een dergelijke bevoegdheid bij de toezichthoudende autoriteiten berust. Indien, zoals in het onderhavige geval, de nationale wetgeving hierover niets bepaalt, blijft het niettemin de taak van elke autoriteit om de haar door de AVG toegekende opdrachten uit te voeren, teneinde de tekst een nuttig effect te geven[6].

29. Het Algemeen Secretariaat, dat onder meer tot uitvoerende taak heeft adviezen uit te brengen in het kader van de GEB (artikel 20, § 1, 3°, van de WOG), beschikt over de nodige ervaring om de risico's te beoordelen die verbonden zijn aan gegevensverwerkingen door verwerkingsverantwoordelijken. Bovendien heeft het de uitvoerende taak om toe te zien op technologische ontwikkelingen die een impact hebben op de bescherming van persoonsgegevens (artikel 20, § 1, 3° van de WOG), wat een opvolging vereist van de technologieën die door hackers worden gebruikt en die kunnen worden beschreven in de formulieren voor de melding van een gegevensinbreuk.

30. Het Algemeen Secretariaat is in feite een afdeling van de GBA met bijzondere expertise in het analyseren van de risico's die voortvloeien uit een aan de GBA gemelde gegevensinbreuk.

31. Anderzijds heeft de directeur van het Algemeen Secretariaat, net als elke andere directeur, de bevoegdheid om een dossier ter beoordeling voor te leggen aan het

[6] Zie in dit verband de opdrachten die aan toezichthoudende autoriteiten zijn toegekend bij artikel 57.1 van de AVG.

Directiecomité met het oog op een eventuele toepassing van artikel 63, 1°, van de WOG. Gelet op het bovenstaande (punten 29 en 30) blijkt dat de directeur van het Algemeen Secretariaat op basis van zijn analyse van het formulier voor de melding van een gegevensinbreuk bevoegd was – zonder uit te sluiten dat andere directeurs hetzelfde hadden kunnen doen – om een nota aan het Directiecomité voor te leggen in de zin van artikel 4 van het Reglement van interne orde.

32. Bovendien merkt de Geschillenkamer op dat artikel 4 van het RIO de bevoegde directeur weliswaar verplicht het dossier ten minste een week vóór de zitting aan de leden van het Directiecomité te bezorgen, maar dat het RIO de directeur niet verplicht een datum op de nota zelf te vermelden. In het onderhavige geval heeft de GBA de verweerder voorgesteld om vóór de hoorzitting vast te stellen dat deze bepaling van het RIO was nageleefd, aangezien de nota een week vóór de zitting van het Directiecomité per e-mail was verzonden. De verweerder heeft deze datum tijdens de hoorzitting niet betwist.

33. In ieder geval valt deze bepaling onder de interne organisatieregels van de GBA en kan zij niet leiden tot de nietigheid van de procedure, zoals de verweerder betoogt. Deze termijn van orde, die een indicatieve en geen dwingende termijn is, heeft tot doel de directeurs in hun functie te beschermen en niet om rechten toe te kennen aan de partijen in een procedure. Bijgevolg heeft deze termijn geen gevolgen voor derden en kan hij door de verweerder niet worden ingeroepen om de nietigverklaring van de onderhavige procedure te vorderen. Bovendien zij eraan herinnerd dat deze termijn in acht is genomen.

34. **Bij wijze van conclusie kan worden gesteld dat de directeur van het Algemeen Secretariaat de in artikel 4 van het RIO voorgeschreven procedure naar behoren heeft nageleefd door een nota aan het Directiecomité op te stellen. Deze nota is ten minste een week vóór de zitting aan de leden van het Directiecomité bezorgd. De argumenten van de verweerder zijn dan ook ongegrond.**

II.2.2. Proces-verbaal van het Directiecomité:

35. **De verweerder** legt uit dat er twijfel bestaat over het feit dat er een proces-verbaal van de beslissing van het Directiecomité is opgemaakt en ondertekend door de voorzitter van het Directiecomité, wat een inbreuk vormt op artikel 16 van de WOG. Bovendien is hij van oordeel dat niet is aangetoond dat de meerderheid van de leden van het Directiecomité aanwezig was, noch dat een meerderheid van de leden voor heeft gestemd krachtens artikel 3 van het RIO. De verweerder stelt dat evenmin is aangetoond dat de voorzitter van de Geschillenkamer zich heeft onthouden van

deelname aan de stemming van het Directiecomité over dit punt, terwijl hij mogelijk later inhoudelijk over de zaak moet oordelen.

36. **De Geschillenkamer** herinnert eraan dat de processen-verbaal van het Directiecomité tal van onderwerpen behandelen, waaronder strategische beslissingen van de GBA, en dat ze persoonsgegevens bevatten. Overeenkomstig het beginsel van minimale gegevensverwerking (artikel 5.1.c) van de AVG) en met inachtneming van het vertrouwelijkheidsbeginsel dat van toepassing is op de leden van het Directiecomité (artikel 48 van de WOG), worden deze processen-verbaal niet integraal doorgestuurd naar de partijen die bij een procedure betrokken zijn. Zij ontvangen enkel een uittreksel van het desbetreffende proces-verbaal, zodat zij het bestaan ervan kunnen verifiëren voor het gedeelte dat op hen betrekking heeft.

37. Indien een partij vreest dat een formaliteit niet is nageleefd, is de GBA bereid de door een partij gewenste aanvullende informatie te verstrekken, zodat deze partij kan beoordelen of de betwiste formaliteiten zijn nageleefd. Een dergelijke mogelijkheid werd de verweerder vóór de hoorzitting geboden, zodat hij kon vaststellen dat de GBA de formaliteiten had nageleefd die hij aanvoerde op straffe van nietigheid van de procedure.

38. De verweerder heeft in het proces-verbaal kunnen vaststellen dat alle leden van het Directiecomité bij de beraadslaging aanwezig waren, dat er geen bezwaar van een van de leden van het Directiecomité is genoteerd en dat het proces-verbaal wel degelijk door de voorzitter van het Directiecomité is ondertekend. Hij kon ook vaststellen dat het Directiecomité had besloten de Inspectiedienst in te schakelen op grond van artikel 63, 1°, van de WOG. Het argument van de verweerder om het bestaan van een proces-verbaal en de naleving van de vormvoorschriften ervan te betwisten, is dus niet geldig.

39. Volgens vaste rechtspraak kan kritiek op partijdigheid niet worden gebaseerd op een situatie die voortvloeit uit de normale toepassing van de wet (zie in die zin het arrest van de Raad van State van 11 mei 2021[7]). Het Directiecomité bestaat uit de voorzitter van de Geschillenkamer (artikel 12 van de WOG). Het Directiecomité is ook bevoegd om de Inspectiedienst in te schakelen bij de vaststelling van ernstige aanwijzingen voor het bestaan van een praktijk die aanleiding kan geven tot een inbreuk op de grondbeginselen van de bescherming van persoonsgegevens (artikel 63, 1°, van de WOG).

[7] Zie het arrest van de Raad van State van 11 mei 2021, nr. 250.571, (enkel in het Frans) beschikbaar via de volgende link: http://www.raadvst-consetat.be/Arrets/250000/500/250571.pdf#xml=http://www.raadvst-consetat.be/apps/dtsearch/getpdf.asp?DocId=39004&Index=c%3a%5csoftware%5cdtsearch%5cindex%5carrets%5ffr%5c&HitCount=2&hits=16+17+&083572024517.

40. Geen enkel artikel van de WOG voorziet in een uitzondering met betrekking tot de deelname van de voorzitter van de Geschillenkamer aan de beslissingen van het Directiecomité. Wanneer de voorzitter van de Geschillenkamer van een rol of functie wordt uitgesloten, wordt dit uitdrukkelijk in de wet bepaald (zie de artikelen 13 en 18 van de WOG), wat aantoont dat de wetgever niet de bedoeling had om de voorzitter van de Geschillenkamer uit te sluiten van deelname aan de beraadslagingen van het Directiecomité. Hij is dus bevoegd om deel te nemen aan de beraadslagingen van het Directiecomité (artikel 16 van de WOG) en om een beslissing ten gronde te nemen (artikel 98 e.v. van de WOG).

41. De Geschillenkamer herinnert eraan dat zij in het onderhavige geval collegiaal, dat wil zeggen met drie leden, zitting houdt. Zij herinnert eraan dat het Directiecomité bij zijn beraadslaging over deze procedure eveneens met vijf leden zitting hield. In dergelijke collegiale situaties herinnert het Marktenhof eraan dat zelfs indien de partijdigheid van een lid zou worden aangetoond, dit op zich geen invloed heeft op de rechtmatigheid van de bestreden beslissing[8].

42. Ten slotte moet de vermeende partijdigheid van een collegiaal orgaan concreet worden aangetoond, wat inhoudt dat specifieke feiten of gedragingen met betrekking tot dat orgaan, en dus door zijn leden, aan het licht moeten worden gebracht[9] . Wat de leden van het Directiecomité en de Geschillenkamer betreft, bepaalt artikel 43, § 2, van de WOG uitdrukkelijk het volgende: "Het is hen verboden aanwezig te zijn bij een beraadslaging of besluit over dossiers waarbij zij een persoonlijk of rechtstreeks belang hebben of waarbij hun bloed- of aanverwanten tot en met de derde graad een persoonlijk of rechtstreeks belang hebben." Deze situaties van partijdigheid zijn bij wet geregeld.

43. Hoewel de wetgever geen specifieke wrakingsregeling heeft voorzien om de onafhankelijkheid en onpartijdigheid van de leden van de Geschillenkamer te waarborgen[10], is de Geschillenkamer bereid om in te gaan op ernstige argumenten van partijen met betrekking tot de partijdigheid van deze leden. In het onderhavige geval heeft de verweerder geen aanwijzingen voor partijdigheid van de voorzitter van de Geschillenkamer aangevoerd die zijn wraking zouden kunnen rechtvaardigen.

---

[8] Hof van Beroep Brussel, sectie Marktenhof, 19de kamer A, arrest van 7 december 2022, (enkel in het Frans) beschikbaar via de volgende link: https://www.gegevensbeschermingsautoriteit.be/publications/arrest-van-7-december-2022-van-het-marktenhof-ar-556-beschikbaar-in-het-frans.pdf.

[9] Hof van Beroep Brussel, sectie Marktenhof, 19de kamer A, Marktenhof, arrest van 7 december 2022, (enkel in het Frans) beschikbaar via de volgende link: https://www.gegevensbeschermingsautoriteit.be/publications/arrest-van-7-december-2022-van-het-marktenhof-ar-556-beschikbaar-in-het-frans.pdf.

[10] Marktenhof, arrest van 31 oktober 2023, nr. 2023/AR/821.

44. **Bij wijze van conclusie kan worden gesteld dat noch de geldigheid van het proces-verbaal van het Directiecomité, noch de deelname van de voorzitter van de Geschillenkamer aan de beraadslaging kan worden betwist. De procedure voldeed aan de wettelijke vereisten en er is geen bewijs van partijdigheid geleverd.**

II.2.3. Ernstige aanwijzingen die door het Directiecomité in aanmerking zijn genomen:

45. **De verweerder** stelt dat de aanwijzingen die het Directiecomité in aanmerking heeft genomen om vast te stellen dat er ernstige aanwijzingen waren voor het bestaan van een praktijk die aanleiding kan geven tot een inbreuk op de grondbeginselen van de bescherming van persoonsgegevens, onjuist zijn. Hij betwist dat de motivering van het Directiecomité mag steunen op een verwijzing naar de nota van het Algemeen Secretariaat. Ten slotte legt hij uit dat het feit dat het ziekenhuis het slachtoffer werd van een cyberaanval niet het gevolg is van een schending van zijn kant en geen ernstige aanwijzing vormt in de zin van artikel 63, 1°, van de WOG.

46. **De Geschillenkamer** herinnert eraan dat het, op grond van de aan het Directiecomité toegekende bevoegdheden, aan het Directiecomité toekomt om vast te stellen of er ernstige aanwijzingen zijn voor het bestaan van praktijken die aanleiding kunnen geven tot een inbreuk op de grondbeginselen van de bescherming van persoonsgegevens (artikel 63, 1°, van de WOG). Zoals het Marktenhof heeft opgemerkt, gaat het hier om een discretionaire bevoegdheid van de GBA[11].

47. De Raad van State aanvaardt de motivering door verwijzing, op voorwaarde dat het stuk waarnaar wordt verwezen deel uitmaakt van het dossier, wat in dit geval zo is (arrest van de Raad van State van 7 mei 2013, nr. 223.440). De beslissing van het Directiecomité verwijst immers naar de nota die aan het Directiecomité werd bezorgd, en steunt op die nota om de volgende aanwijzingen in aanmerking te nemen:

    a. de storing van het computernetwerk van het ziekenhuis, die heeft geleid tot de annulering van geplande operaties en raadplegingen, alsook tot de sluiting van de spoedeisende hulp;

    b. de gevoeligheid van de gegevens die bij de inbreuk betrokken waren, waaronder met name het nationaal nummer, het identificatienummer van de sociale zekerheid, genetische en biometrische gegevens, gegevens over gezondheid, zorg, seksueel

[11] Hof van Beroep Brussel, sectie Marktenhof, 19de kamer A, Marktenhof, arrest van 22 februari 2022, (enkel in het Frans) beschikbaar via de volgende link: https://www.autoriteprotectiondonnees.be/publications/arret-du-22-fevrier-2023-de-la-cour-des-marches-ar-953.pdf, p. 40 e.v.

gedrag of seksuele gerichtheid, strafrechtelijke veroordelingen, uittreksels uit het strafregister, de inhoud van elektronische communicatie en financiële gegevens;

c. de vermelding in het formulier van de mogelijke impact van de gegevensinbreuk op de rechten en vrijheden van de betrokkenen, zoals de onbeschikbaarheid van gegevens of verwerkingen, waardoor de voortzetting van de verwachte dienstverlening werd verhinderd;

d. het grote aantal betrokkenen, namelijk mogelijk 300.000 personen;

e. het bestaan van een eerdere grote gegevensinbreuk van het type "ransomware" op [datum] 2019. Wat dit punt betreft, heeft de verweerder bevestigd dat er geen losgeld is betaald.

48. Deze informatie was gebaseerd op de beschrijving van de gegevensinbreuk, zoals opgenomen in de initiële en aanvullende meldingsformulieren die het ziekenhuis aan de GBA had toegezonden. Pas door het onderzoek dat later door de Inspectiedienst werd uitgevoerd, kon laatstgenoemde de omvang van deze inbreuk en van de eerdere inbreuk van 2019 enigszins relativeren.

49. Het onderzoek heeft echter geen volledig licht geworpen op de precieze omstandigheden van de inbreuk (zie punt 106 en volgende met betrekking tot het bewaren van logbestanden). Hoe dan ook, indien via deze meldingen onjuiste informatie aan de GBA is verstrekt, kan het Directiecomité niet worden verweten dat het zich daarop heeft gebaseerd om ernstige aanwijzingen vast te stellen die het instellen van een onderzoek rechtvaardigen. Op het moment van de beslissing van het Directiecomité, en op basis van de elementen waarover het beschikte bij de lezing van de initiële melding, heeft het Directiecomité soeverein vastgesteld dat er ernstige aanwijzingen waren die het instellen van een onderzoek rechtvaardigden. De Geschillenkamer kan de beslissing van het Directiecomité slechts aan een marginale controle onderwerpen. In het onderhavige geval heeft het Directiecomité bij de beoordeling van de ernst van de aanwijzingen in kwestie zijn bevoegdheden niet overschreden.

50. Bovendien betwist de verweerder dat het Directiecomité rekening heeft gehouden met een eerdere gegevensinbreuk die in 2019 bij hetzelfde ziekenhuis plaatsvond. Het Directiecomité had echter het recht om zich te baseren op de informatie die de GBA ter beschikking was gesteld via de formulieren voor de melding van een gegevensinbreuk die het ziekenhuis had ingediend. Deze formulieren vormen een essentiële en legitieme bron van informatie voor de GBA, aan de hand waarvan ernstige aanwijzingen voor mogelijke inbreuken op de wetgeving inzake gegevensbescherming kunnen worden geïdentificeerd. Het herhaaldelijk voorkomen van gegevensinbreuken binnen dezelfde instelling, in het bijzonder wanneer deze met

korte tussenpozen plaatsvinden en hoge risico's voor de rechten en vrijheden van de betrokkenen met zich meebrengen, versterkt redelijkerwijs het bestaan van ernstige aanwijzingen in de zin van artikel 63, 1°, van de WOG.

51. Het Directiecomité was soeverein van oordeel dat het feit dat een ziekenhuis binnen twee jaar tijd twee gegevensinbreuken heeft ondergaan, die elk "grote" risico's inhouden voor de rechten en vrijheden van de betrokkenen, een bijkomende ernstige aanwijzing vormt voor het bestaan van praktijken die aanleiding kunnen geven tot een inbreuk op de grondbeginselen van de bescherming van persoonsgegevens.

52. Bovendien lijkt de verweerder het begrip "ernstige aanwijzingen" te verwarren met de vaststelling van een inbreuk op de AVG. Het Directiecomité is niet bevoegd om een inbreuk op de AVG vast te stellen, en een dergelijke vaststelling is niet vereist om artikel 63, 1°, van de WOG te kunnen toepassen. De bevoegdheid om een inbreuk op de AVG vast te stellen, is voorbehouden aan de Geschillenkamer. Pas wanneer zij over een volledig dossier beschikt, dat de conclusies van de partijen en een eventueel onderzoeksverslag bevat, kan de Geschillenkamer bepalen of een cyberaanval een inbreuk op de AVG vormt[12]. Op het moment dat artikel 63, 1°, wordt toegepast, is alleen het bestaan van ernstige aanwijzingen vereist, wat soeverein is beoordeeld (zie de punten 49 tot en met 51 hierboven).

53. **Bij wijze van conclusie kan worden gesteld dat het Directiecomité op basis van de door de verweerder verstrekte informatie terecht heeft vastgesteld dat de ernst van de aanwijzingen in kwestie voldoende was (artikel 63, 1°, van de WOG).**

II.2.4. Doorgifte van het meldingsformulier binnen de afdelingen van de GBA:

54. **De verweerder** is van oordeel dat het formulier voor de melding van een gegevensinbreuk niet binnen de afdelingen van de GBA hoeft te worden gedeeld, aangezien er geen wettelijke bepaling is die dit voorschrijft. Bovendien stelt hij dat noch de AVG, noch de WOG voorziet in de mogelijkheid dat een dergelijke melding aanleiding kan geven tot een procedure voor de Geschillenkamer. Ten slotte voert hij aan dat het Europees Comité voor gegevensbescherming (hierna "EDPB") niet bepaalt dat een dergelijke melding mag worden gebruikt om de inschakeling van de Inspectiedienst te rechtvaardigen of om de melder andere schendingen te verwijten.

55. **De Geschillenkamer** betwist de argumenten die in de conclusie van de verweerder worden aangevoerd en herinnert eraan dat de AVG in artikel 33.1 bepaalt dat "indien

[12] Geschillenkamer, beslissing ten gronde 170/2023 van 20 december 2023, beschikbaar via de volgende link: https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-170-2023.pdf.

een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, [...] de verwerkingsverantwoordelijke deze (...) aan de (...) bevoegde toezichthoudende autoriteit [meldt] (...)". Bovendien geldt het volgende: "Die kennisgeving kan ertoe leiden dat de toezichthoudende autoriteit optreedt overeenkomstig haar in deze verordening neergelegde taken en bevoegdheden." (overweging 87 van de AVG).

56. Bijgevolg is elke toezichthoudende autoriteit wettelijk bevoegd om kennis te nemen van de inhoud van een formulier voor de melding van een gegevensinbreuk dat haar is toegezonden. In tegenstelling tot wat in het verweer wordt aangevoerd, bepaalt de AVG wel degelijk dat een dergelijke melding een autoriteit ertoe kan brengen gebruik te maken van haar onderzoeks- en vervolgingsbevoegdheden. Gelet op de structuur van de GBA rechtvaardigt deze omstandigheid noodzakelijkerwijs de mogelijkheid tot doorgifte van het formulier tussen haar bevoegde diensten.

57. Zelfs indien de verweerder van oordeel is dat overweging 87 van de AVG niet voldoende expliciet is, herinnert de Geschillenkamer eraan dat wanneer een bepaling van het recht van de Europese Unie ("EU") voor meerdere interpretaties vatbaar is, voorrang moet worden gegeven aan de interpretatie die het nuttige effect ervan waarborgt, overeenkomstig de algemene beginselen van het EU-recht[13]. De interpretatie van het EU-recht moet zodanig gebeuren dat de doeltreffendheid van het rechtsstelsel van de EU wordt gewaarborgd en wordt voorkomen dat de bepalingen hun betekenis verliezen[14]. Het argument van de verweerder dat de GBA het formulier voor de melding van een gegevensinbreuk niet mocht doorgeven aan de afdelingen die bij de opvolging van de onderhavige zaak betrokken waren, is dan ook ongegrond.

58. Ten slotte bevestigen de Richtsnoeren van de EDPB voor de berekening van administratieve geldboeten krachtens de AVG[15], in tegenstelling tot wat de verweerder beweert, dat de toezichthoudende autoriteit gebruik kan maken van een aan haar doorgegeven melding van een gegevensinbreuk. In deze richtsnoeren wordt uitdrukkelijk bepaald dat wanneer de toezichthoudende autoriteit via een melding van een gegevensinbreuk kennis heeft gekregen van een inbreuk die de oplegging van

---

[13] Artikel "Le droit de l'Union européenne devant les juridictions de l'ordre judiciaire", Jérémie Van Meerbeeck, Université Catholique de Louvain, 22 september 2015, punt 11.

[14] Zie de arresten van het HvJEG (voorganger van het HvJ-EU), 4 december 1974, Van Duyn, zaak 41/74 en 3 april 2008, Endendijk, zaak C-187/07, punten 14-26.

[15] Zie in dit verband punt 98 van de Richtsnoeren 04/2022 van de EDPB voor de berekening van administratieve geldboeten krachtens de AVG, die op dit punt een standpunt overnemen dat is vastgelegd in de Richtsnoeren voor de toepassing en vaststelling van administratieve geldboeten WP253, onderschreven door de EDPB tijdens zijn eerste plenaire vergadering van 25 mei 2018, beschikbaar via de volgende link: https://www.edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_nl_0.pdf.

een geldboete rechtvaardigt, deze factor als neutraal moet worden beschouwd bij de berekening van de geldboete.

59. **Bij wijze van conclusie kan worden gesteld dat het formulier voor de melding van een gegevensinbreuk op geldige wijze is gedeeld binnen de afdelingen van de GBA, zodat zij gebruik kunnen maken van hun onderzoeks- en vervolgingsbevoegdheden.**

II.3. Over de inhoud

II.3.1. Vaststelling 1: over de gegevensbeschermingseffectbeoordeling

60. *Ten eerste* stelt **de verweerder** dat, aangezien alleen de verwerking van de e-mailberichten van het personeel door de gegevensinbreuk was getroffen, hij niet verplicht was om voor deze verwerking een GEB uit te voeren, aangezien deze verwerking geen gevoelige gegevens omvat. Tijdens de hoorzitting heeft de Geschillenkamer de verweerder nader bevraagd over zijn redenering dat er bij de verwerking van de e-mailberichten van het ziekenhuispersoneel geen gevoelige gegevens aan bod komen. De verweerder stelde dat er waarschijnlijk wel gevoelige gegevens via e-mailberichten werden uitgewisseld, maar verklaarde dat deze gevoelige gegevens versleuteld waren.

61. *Ten tweede* stelt hij dat het uitvoeren van een GEB geen specifieke vorm hoeft aan te nemen en dat het onjuist is te stellen dat er geen GEB is uitgevoerd, aangezien het ziekenhuis beveiligingsmaatregelen heeft getroffen die het resultaat zijn van risicoanalyses.

62. *Ten derde* stelt hij dat, aangezien de verwerking vóór de inwerkingtreding van de AVG in mei 2018 is uitgevoerd, hij niet onderworpen is aan de verplichting om een GEB uit te voeren, en dat zelfs indien dit wel het geval zou zijn, hij zou zijn vrijgesteld van deze verplichting dankzij de door de EDPB toegekende "respijtperiode" van drie jaar.

63. *Ten eerste* herinnert **de Geschillenkamer** eraan dat een GEB in verschillende gevallen vereist is, met name bij grootschalige verwerking van bijzondere categorieën van gegevens (artikel 35.3.b) van de AVG). Een GEB moet ten minste het volgende bevatten (artikel 35.7 en overwegingen 84 en 90 van de AVG):

a. een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;

b. een beoordeling van de noodzaak en de evenredigheid van de verwerkingen;

c. een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;

d. de beoogde maatregelen om:

i. de risico's aan te pakken;

ii. aan te tonen dat aan de AVG is voldaan.

64. In het onderhavige geval verwerkt de verwerkingsverantwoordelijke op grote schaal (300 000 patiënten in de databank) gevoelige gegevens (met name gezondheidsgegevens en genetische gegevens) van kwetsbare personen (patiënten), waardoor hij aan deze verplichting moet voldoen. De Geschillenkamer herinnert eraan dat een van de voordelen van het uitvoeren van een GEB is dat de verwerkingsverantwoordelijke preventief beveiligingslekken kan opsporen en passende maatregelen kan treffen om persoonsgegevens tegen gegevensinbreuken te beschermen.

65. In tegenstelling tot wat de verweerder beweert, ontslaat het feit dat de aanval zich concentreerde op de mailboxen van het personeel en niet op de medische dossiers van de patiënten, de verweerder niet van zijn plicht om een GEB uit te voeren. De Geschillenkamer herinnert eraan dat de definitie van "verwerking" in de zin van de AVG ruim is en met name het bewaren, verzamelen, raadplegen, gebruiken en ter beschikking stellen van persoonsgegevens omvat (artikel 4 van de AVG). Ook al was de aanval alleen gericht op de mailboxen van het personeel, het feit dat hiermee op grote schaal gevoelige gegevens van kwetsbare personen kunnen worden verwerkt, verplicht de verweerder ertoe om te voldoen aan zijn verplichting om een GEB uit te voeren met betrekking tot deze verwerking, ongeacht of deze gegevens tijdens het verzenden van e-mailberichten worden versleuteld. Hoe dan ook beperkt deze vaststelling zich niet tot de beoordeling van de uitvoering van een GEB met betrekking tot uitsluitend de specifieke verwerking die verband houdt met de mailboxen van het personeel[16].

66. Bovendien lijkt het niet relevant dat de verweerder beweert dat alleen de mailboxen van het personeel zijn getroffen, aangezien uit het onderzoeksverslag blijkt dat de servers van het ziekenhuis zijn verstoord (waaronder de software die de medische dossiers ondersteunt) en dat het ziekenhuis als gevolg van de aanval niet meer operationeel was. Bovendien blijkt uit het onderzoek duidelijk dat er aanwijzingen zijn gevonden op de "radiologieserver". In de conclusie van de verweerder staat het volgende (vrije vertaling): "Het ziekenhuis heeft zijn diensten geleidelijk maar snel en zonder risico's kunnen hervatten, met inbegrip van de radiologiedienst.", en "Ten slotte heeft grondig onderzoek door het ziekenhuis en de dienstverleners waarop het een beroep heeft gedaan, aangetoond dat tijdens de aanval slechts 5 gigabyte aan

[16] Overeenkomstig artikel 35.1 van de AVG is het aan de verwerkingsverantwoordelijke om te beoordelen of het opportuun is om een of meer GEB's uit te voeren: "Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden."

informatie van een van de servers van het ziekenhuis naar het internet is geëxporteerd. De server in kwestie bevat echter alle röntgenfoto's (...)." De gegevensinbreuk had dus wel degelijk betrekking op gevoelige categorieën van persoonsgegevens, in dit geval de op grote schaal verwerkte gezondheidsgegevens van de patiënten van het ziekenhuis.

67. *Ten tweede* is het onjuist te stellen dat de GEB geen specifieke vorm hoeft aan te nemen, aangezien het verantwoordingsbeginsel van de AVG vereist dat verwerkingsverantwoordelijken kunnen aantonen dat zij aan hun verplichtingen voldoen (artikelen 5.2 en 24 van de AVG) en artikel 35.7 van de AVG de minimale inhoud van een GEB opsomt. Hieruit volgt dat de GEB moet worden uitgevoerd in een afzonderlijk document dat niet mag worden verward met andere eventuele risicoanalyses. De risicoanalyses die de verweerder heeft voorgelegd, voldoen niet aan de vereisten die nodig zijn opdat de Geschillenkamer zou kunnen vaststellen dat er daadwerkelijk een GEB bestaat.

68. In ieder geval heeft de verweerder in zijn antwoorden op de vragen van de Inspectiedienst bevestigd dat de verwerkingsverantwoordelijke geen GEB heeft uitgevoerd. Het feit dat de auditors van het ziekenhuis risicoanalyses hebben uitgevoerd en dat een GEB is aangevraagd, volstaat voor de Geschillenkamer niet om aan te nemen dat de verweerder een GEB heeft uitgevoerd.

69. *Ten derde* voert de verweerder ten onrechte aan dat, aangezien de verwerking vóór de inwerkingtreding van de AVG in mei 2018 is uitgevoerd, hij niet onderworpen is aan de verplichting om een GEB uit te voeren. Wat betreft verwerkingen die vóór de inwerkingtreding van de AVG zijn uitgevoerd, herinnert de Geschillenkamer eraan dat de EDPB het volgende aangeeft: "De vereiste om een gegevensbeschermingseffectbeoordeling uit te voeren, geldt voor bestaande verwerkingen [*die vóór de AVG zijn uitgevoerd*] die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen en waarvoor de risico's zijn veranderd, rekening houdend met de aard, de omvang, de context en de doeleinden van de verwerking." (onderstreping en informatie tussen haakjes toegevoegd door de Autoriteit)[17]

70. Aangezien de risico's in de ziekenhuissector voortdurend veranderen (wat door de verweerder niet wordt betwist)[18] en een blokkering van de activiteiten van een

[17] Zie de Richtsnoeren van de EDPB voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679, beschikbaar via de volgende link: https://ec.europa.eu/newsroom/article29/items/611236/en (pagina 16).

[18] De verweerder stelt zelf in zijn conclusie dat ziekenhuizen onderhevig zijn aan specifieke en voortdurend veranderende risico's (vrije vertaling): "(...) ziekenhuisstructuren zijn een geliefkoosd doelwit voor hackers" en "hackers zijn talrijk, beschikken over onuitputtelijke middelen en richten zich in het bijzonder op ziekenhuisgroepen".

ziekenhuis een groot risico vormt voor de rechten en vrijheden van natuurlijke personen[19], verwerpt de Geschillenkamer het argument dat het ziekenhuis zou zijn vrijgesteld van de verplichting om een GEB uit te voeren.

71. Ten slotte betwist de Geschillenkamer de beweringen van de verweerder die tijdens de hoorzitting werden geuit, namelijk dat de EDPB een respijtperiode van drie jaar zou hebben toegekend voor het uitvoeren van GEB's voor bestaande verwerkingen na de inwerkingtreding van de AVG. Indien een dergelijke respijtperiode al werd toegestaan door nationale autoriteiten onder specifieke voorwaarden – zoals de Commission Nationale de l'Informatique et des Libertés (CNIL) in Frankrijk – dan geldt dit niet voor de EDPB, die geen dergelijke termijn heeft toegekend. In ieder geval beschikte het ziekenhuis meer dan drie jaar na de inwerkingtreding van de AVG, namelijk op 25 mei 2018[20], nog steeds niet over een GEB. Het argument met betrekking tot het bestaan van een vermeende respijtperiode – *quod non* – is dan ook niet overtuigend.

72. **Bij wijze van conclusie kan worden gesteld dat de verweerder zijn verplichting om een GEB uit te voeren in de zin van artikel 35.3 van de AVG niet is nagekomen.**

II.3.2. Vaststelling 2: over het effectief en formeel beleid voor informatieveiligheid

73. *Ten eerste* voert **de verweerder** aan dat de GBA niet bevoegd is om toe te zien op de naleving van de verplichting tot toepassing van de minimale normen inzake informatieveiligheid en privacy voor de instellingen van sociale zekerheid krachtens artikel 2, eerste lid, 2°, van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid (hierna "minimale normen")[21]. *Ten tweede* stelt hij dat de AVG geen formele verplichting bevat om over een beleid voor informatieveiligheid te beschikken, en *a fortiori* geen vormvoorschriften oplegt voor een dergelijk beleid. Hij legt uit dat het beleid voor informatieveiligheid van het ziekenhuis in dit geval moet worden gezien als een onderdeel van een reeks documenten en procedures die zijn ingesteld en die de organisatorische en technische maatregelen van het ziekenhuis vormen.

---

[19] Zoals vermeld in de Richtsnoeren van de WP29 voor de melding van inbreuken in verband met persoonsgegevens: "In de context van een ziekenhuis kan de onbeschikbaarheid van cruciale medische gegevens over patiënten, zelfs tijdelijk, een risico voor de rechten en vrijheden van natuurlijke personen inhouden. Het kan bijvoorbeeld tot gevolg hebben dat operaties worden geannuleerd en dat levens in gevaar komen." Deze Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 zijn gepubliceerd door de WP29 (voorganger van de EDPB). Ze zijn te raadplegen via de volgende link: https://ec.europa.eu/newsroom/article29/items/612052/en (zie pagina 9).

[20] De AVG is op 25 mei 2018 in werking getreden, terwijl de aanval plaatsvond op [...] 2021, meer dan drie jaar later.

[21] De minimale normen informatieveiligheid en privacy, in de versie van 7 maart 2017, zijn beschikbaar via deze link: https://www.ksz-bcss.fgov.be/sites/default/files/assets/gegevensbescherming/mnm_minimale_normen_v2017.pdf.

74. *Ten eerste* herinnert **de Geschillenkamer** eraan dat het krachtens artikel 32.1 van de AVG de taak is van de GBA om toe te zien op de naleving van passende technische en organisatorische maatregelen, rekening houdend met "de stand van de techniek". De bovengenoemde minimale normen, die bindend zijn voor instellingen van sociale zekerheid op het vlak van gegevensbeveiliging in België, vormen een nuttig referentiepunt voor "de stand van de techniek" waarop de Geschillenkamer zich kan beroepen. In deze normen staat immers het volgende: "Daarnaast is het nuttig om deze normen ook toe te passen op informatieveiligheid en privacy in de ruime betekenis (...)."[22]

75. Bovendien stelt de Geschillenkamer vast dat het beleid voor informatieveiligheid van 2022 van het ziekenhuis (zie punt 78) de verplichting bevat om de minimale normen na te leven. De niet-naleving door de verweerder van de beveiligingsverplichtingen die in deze minimale normen zijn opgenomen, vormt dus op zich een schending van de technische en organisatorische maatregelen die de verweerder geacht wordt te hebben getroffen. De inleidende opmerking van de verweerder is dan ook niet gegrond en de Geschillenkamer zal in haar overwegingen rekening houden met de minimale normen.

76. *Ten tweede* herinnert de Geschillenkamer eraan dat de AVG de verwerkingsverantwoordelijke verplicht om persoonsgegevens zodanig te verwerken dat een passende beveiliging ervan is gewaarborgd, door middel van passende technische of organisatorische maatregelen (artikel 5.1.f) van de AVG), hierna de "beginselen van integriteit en vertrouwelijkheid" genoemd. Artikel 32 van de AVG bevat meer details over deze technische en organisatorische maatregelen, bijvoorbeeld de verplichting voor de verwerkingsverantwoordelijke om ervoor te zorgen dat deze maatregelen een op het risico afgestemd beveiligingsniveau waarborgen. Daarnaast bepaalt artikel 5.2 van de AVG het volgende: "De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen." Dit beginsel wordt het verantwoordingsbeginsel genoemd.

77. Zij merkt op dat de verweerder haar talrijke documenten heeft toegezonden die, in hun geheel genomen, het bestaan van een beleid voor informatieveiligheid van het

---

[22] Zie de bovengenoemde minimale normen, beschikbaar via de volgende link: https://www.ksz-bcss.fgov.be/sites/default/files/assets/gegevensbescherming/mnm_minimale_normen_v2017.pdf, pagina 3, waarvan de volledige passage hierna wordt weergegeven: "*Daarnaast is het nuttig om deze normen ook toe te passen op informatieveiligheid en privacy in de ruime betekenis zoals gedefinieerd in het koninklijk besluit van 17 maart 2013 betreffende de veiligheidsadviseurs ingevoerd door de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator, en zoals overgenomen in het koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid: "Strategie, regels, procedures en middelen voor het beschermen van alle soorten informatie zowel in de transmissiesystemen als in de verwerkingssystemen om de vertrouwelijkheid de beschikbaarheid, de integriteit, de betrouwbaarheid, de authenticiteit en de onweerlegbaarheid ervan te garanderen".*"

ziekenhuis zouden moeten aantonen (bijvoorbeeld het arbeidsreglement van het ziekenhuispersoneel, het ZNP, enz.).

78. **Het beleid voor informatieveiligheid van 3 maart 2022**: de Geschillenkamer neemt nota van de toezending van het bovengenoemde beleid voor informatieveiligheid, waarvan de eerste versie dateert van 3 maart 2022. Tijdens de hoorzitting heeft de verweerder bevestigd dat het beleid voor informatieveiligheid vóór die datum bestond uit een reeks documenten (zie punt 84). Het opstellen van een reeks documenten zonder onderlinge samenhang of verwijzingen, en met doeleinden die geen verband houden met de implementatie van technische en organisatorische maatregelen zoals voorgeschreven door de AVG, vormt echter geen "passende technische en organisatorische maatregelen" om de risico's aan te pakken, in de zin van artikel 32.1 van de AVG. Bovendien bepalen de minimale normen waarnaar het beleid voor informatieveiligheid van 2022 verwijst, dat er een formeel beleid moet zijn: "Elke organisatie moet over een formeel, geactualiseerd en door de verantwoordelijke voor het dagelijkse bestuur (of gelijkwaardig), goedgekeurd beleid voor informatieveiligheid beschikken." (onderstreept door de Autoriteit)

79. De Geschillenkamer merkt op dat dit zeer algemene beleid zelf vermeldt dat het om een "basisdocument" gaat. In dit basisdocument wordt het volgende opgelegd: "Een duidelijk en helder beleid rond informatieveiligheid en privacy opzetten, valideren, communiceren en onderhouden om de beschikbaarheid, de integriteit, de vertrouwelijkheid te garanderen in lijn met de doelstellingen van Y."

80. De Geschillenkamer merkt overigens op dat dit basisdocument na de gegevensinbreuk is opgesteld en dat het door de Geschillenkamer niet kan worden beschouwd als een rechtvaardiging voor het bestaan van een dergelijk beleid op het moment van de gegevensinbreuk. Bovendien is het geen exhaustief of definitief document, in die zin dat het voor de verduidelijking van de toepassing ervan verwijst naar andere documenten. Dit basisdocument volstaat op zichzelf niet om volledig te voldoen aan de vereisten voor het treffen van passende organisatorische maatregelen in de zin van artikel 32.1 van de AVG, en is bovendien pas na de inbreuk opgesteld.

81. **Het duidelijk en helder beleid voor informatieveiligheid en privacy:** de verweerder heeft tijdens de hoorzitting bevestigd dat het "duidelijk en helder" beleid voor informatieveiligheid, dat hij volgens het bovengenoemde basisdocument had moeten invoeren, niet is ingevoerd. Hij blijft er bovendien bij dat zijn beveiligingsbeleid bestaat uit een reeks documenten (zie punt 84).

82. De Geschillenkamer stelt vast dat het doel van dit duidelijk en helder beleid was om in detail in te gaan op de uitvoering van de technische en organisatorische maatregelen

van de verweerder. In het beleid voor informatieveiligheid van 3 maart 2022 staat immers het volgende (vrije vertaling): "In de volgende paragrafen worden, zonder in detail te treden over de uitvoering, de belangrijkste beheersmaatregelen voor het beheer van de informatieveiligheid van Y uiteengezet." De Geschillenkamer stelt vast dat zij, bij gebrek aan dit duidelijk en helder beleid, niet in staat is om de technische en organisatorische maatregelen die in overeenstemming met de doelstellingen van Y zijn uitgevoerd, volledig te beoordelen.

83. De Geschillenkamer is van oordeel dat de invoering van een reeks documenten zoals beschreven in punt 77 niet voldoet aan de voorwaarde om "passende technische en organisatorische maatregelen" te treffen. De invoering van een "duidelijk en helder beleid" zou aan deze voorwaarde hebben voldaan, *quod non*. Zij stelt dan ook een schending vast van artikel 32.1 van de AVG.

84. **De door de verweerder overgelegde documenten:** de meeste overgelegde documenten zijn na de tweede gegevensinbreuk opgesteld. Hun nut in het kader van deze procedure is dan ook beperkt tot de invloed die deze late opstelling zou hebben op de vaststelling van een eventuele sanctie, in het bijzonder de beoordeling van het bedrag van een mogelijke geldboete. Zij stellen de Geschillenkamer niet in staat om te beoordelen in hoeverre de verweerder op het moment van de tweede gegevensinbreuk voldeed aan de beginselen van integriteit en vertrouwelijkheid en aan de beveiligingsvereisten van de AVG.

85. Wat betreft de officiële documenten waarvan de datum aantoont dat zij ten tijde van de tweede inbreuk waren ingevoerd, merkt de Geschillenkamer op dat geen van deze documenten bedoeld is om aan te tonen dat het ziekenhuis voldoet aan de artikelen 5.1.f) en 32 van de AVG. De GBA herinnert er in dit verband aan dat de verwerkingsverantwoordelijke moet kunnen aantonen dat de in artikel 5.1 van de AVG uiteengezette beginselen worden nageleefd.

86. Het ZNP heeft bijvoorbeeld tot doel procedures vast te stellen voor een doeltreffende opvang van een plotselinge toestroom van patiënten, zonder dat dit ten koste gaat van de zorg voor de reeds opgenomen patiënten. Het informaticahandvest voor het personeel is een contractuele maatregel waarmee de verwerkingsverantwoordelijke bepaalde verplichtingen kan opleggen aan het ziekenhuispersoneel.

87. De GBA beschouwt dergelijke documenten niet als een beleid voor informatieveiligheid waarmee kan worden aangetoond dat de door de verwerkingsverantwoordelijke vastgestelde technische en organisatorische maatregelen een op het risico afgestemd beveiligingsniveau waarborgen, in overeenstemming met de AVG. Alleen een formeel en geactualiseerd beleid voor informatieveiligheid kan de verwerkingsverantwoordelijke in staat stellen aan te

tonen dat hij voldoet aan de beveiligingsvereisten van de AVG, op voorwaarde dat de inhoud ervan volledig is, daadwerkelijk is afgestemd op het risico en correct wordt geïmplementeerd.

88. **Bij wijze van conclusie kan de verweerder niet aantonen dat hij voldoet aan de artikelen 5.1.f) en 32 van de AVG door middel van een formeel en geactualiseerd beleid voor informatieveiligheid op het moment van de gegevensinbreuk.**

II.3.3. Vaststelling 3: over het beleid en/of de procedure voor het bijwerken van de beveiliging van IT-apparatuur (software)

89. **De verweerder** stelt dat het beleid voor het bijwerken van de beveiliging van IT-apparatuur bestaat uit consultancycontracten die door het ziekenhuis zijn gesloten om een maandelijkse controle van zijn installaties te waarborgen. Bovendien vermeldt hij dat het ziekenhuis na de gegevensinbreuk verschillende maatregelen heeft getroffen, waaronder de installatie van een Web Application Firewall in maart 2022.

90. **De Geschillenkamer** wijst erop dat de verweerder noch in zijn antwoorden aan de Inspectiedienst, noch in zijn conclusie uitlegt welk(e) beleid en/of procedure voor het bijwerken van de beveiliging van IT-apparatuur (software) op het moment van de gegevensinbreuk van kracht was.

91. Uit het onderzoeksverslag blijkt dat het door de hacker misbruikte beveiligingslek te wijten was aan een kwetsbaarheid op de Microsoft Exchange-server. Door misbruik te maken van dit lek kon de hacker zijn aanval uitvoeren en een reeks toegankelijke servers versleutelen. Het feit dat alleen firewalls en antivirusgateways werden gecontroleerd, was niet voldoende om misbruik van dit soort beveiligingslekken te voorkomen.

92. Uit het onderzoek van de Inspectiedienst blijkt dat de kwetsbaarheid die door de hacker werd misbruikt, als "kritiek" werd beschouwd vanwege het gemak waarmee deze kon worden misbruikt. Gelet op de verstrekte antwoorden toont de verweerder niet aan dat dit type risico op het moment van de gegevensinbreuk kon worden opgespoord en beheerd.

93. Naast de beginselen van integriteit en vertrouwelijkheid en de beveiligingsvereisten (artikelen 5.1.f) en 32 van de AVG) verplicht de AVG de verwerkingsverantwoordelijke om de getroffen technische en organisatorische maatregelen te evalueren en indien nodig te actualiseren (artikel 24 van de AVG). De EDPB noemt goed patchbeheer (proper patch management) als een van de belangrijkste beveiligingsmaatregelen in zijn Richtsnoeren 01/2021 van 14 december 2021 over voorbeelden betreffende de

melding van inbreuken in verband met persoonsgegevens (zie punt 18)[23]. De minimale normen herinneren bovendien aan het volgende: "Elke organisatie moet een systeem en formele, geactualiseerde procedures installeren die toelaten om veiligheidsinbreuken te detecteren, op te volgen en te herstellen in verhouding tot het technisch/operationeel risico."

94. Uit het verslag van de Inspectiedienst blijkt dat de verwerkingsverantwoordelijke geen maatregelen had getroffen die hem hadden kunnen waarschuwen dat zijn verwerking van persoonsgegevens geen passende beveiliging bood tegen de risico's. Ondanks de voorschriften van artikel 24 van de AVG en de verplichting voor de verwerkingsverantwoordelijke om aan te tonen dat hij de basisbeginselen van de AVG naleeft overeenkomstig artikel 5.2 van de AVG, toont de verweerder niet aan welke technische en organisatorische maatregelen op het moment van de gegevensinbreuk waren getroffen met betrekking tot de beveiliging van de software, noch hoe deze maatregelen werden geëvalueerd of geactualiseerd.

95. Hoewel de verweerder een groot aantal maatregelen opsomt die zijn getroffen, zijn deze pas na de inbreuk genomen.

96. **Bij wijze van conclusie is de Geschillenkamer van oordeel dat de verweerder op het moment van de gegevensinbreuk niet heeft voldaan aan zijn verplichting om een beleid en/of procedure voor het bijwerken van de beveiliging van IT-apparatuur (software) vast te stellen, en dus in strijd heeft gehandeld met de artikelen 5.1.f), 32 en 24 van de AVG vanwege de ontoereikendheid van deze technische maatregelen en de actualisering daarvan.**

II.3.4. Vaststelling 4: over de andere beveiligingsmaatregelen

Over het opleidings-/bewustmakingsprogramma voor werknemers

97. **De verweerder** stelt dat het ziekenhuis beschikt over een "echt bewustmakingsprogramma voor werknemers" (vrije vertaling), dat met name bestaat uit een opleiding over phishing die werd gegeven na de eerste gegevensinbreuk in 2019, het informaticahandvest dat bij indiensttreding aan werknemers wordt overhandigd, de geheimhoudingsverplichtingen, veiligheidsoefeningen, de opleiding over het ZNP en de deelname van bepaalde werknemers aan de Cyber-Europe-dagen.

---

[23] EDPB, Richtsnoeren 01/2021 over voorbeelden betreffende de melding van inbreuken in verband met persoonsgegevens, vastgesteld op 14 december 2021, v2.0, beschikbaar via de volgende link: https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_nl.pdf.

Zie in dit verband ook de vorige versie van deze richtsnoeren (voor openbare raadpleging) van 14 januari 2021, waarin deze aanbevelingen al worden vermeld in punt 18 (enkel in het Engels beschikbaar): https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.

98. **De Geschillenkamer** herinnert eraan dat artikel 32 van de AVG de verwerkingsverantwoordelijke verplicht om passende technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Artikel 5 vereist dat persoonsgegevens zodanig worden verwerkt dat een passende beveiliging ervan gewaarborgd is. Bovendien bepaalt artikel 24 van de AVG dat de verwerkingsverantwoordelijke deze maatregelen moet evalueren en indien nodig actualiseren.

99. Werknemers van een ziekenhuis die in contact komen met bijzondere categorieën van persoonsgegevens moeten op passende en regelmatige wijze worden opgeleid over de minimale beveiligingsnormen die moeten worden nageleefd bij de verwerking van dergelijke gegevens, afhankelijk van de relevantie voor hun rol of functie.

100. Deze voortgezette opleiding maakt integraal deel uit van de organisatorische maatregelen die het ziekenhuis moet treffen om de beveiliging van gegevens te waarborgen. Zij moet regelmatig worden bijgewerkt om risico's op gegevensinbreuken te voorkomen. In een context waarin ziekenhuizen steeds vaker worden geconfronteerd met cyberaanvallen, is het immers essentieel dat opleidingen up-to-date blijven om te voldoen aan de reglementaire vereisten en om persoonsgegevens doeltreffend te beschermen.

101. In tegenstelling tot wat de verweerder beweert, kan de Geschillenkamer niet aannemen dat het ziekenhuis een echt opleidings-/bewustmakingsprogramma voor werknemers heeft opgezet. Geen van de in punt 97 genoemde documenten vormt, zelfs niet samen, een echt voortgezet en systematisch opleidingsprogramma inzake de AVG zoals vereist door artikel 32 van de AVG. Een opleiding over phishing is weliswaar nuttig, maar volstaat niet om de belangrijke aspecten van de bescherming van persoonsgegevens te dekken.

102. Bovendien volstaan het bij indiensttreding overhandigde informaticahandvest en de geheimhoudingsverplichtingen, zonder regelmatige opvolging en relevante updates, niet om te stellen dat werknemers regelmatig worden geïnformeerd over goede praktijken inzake de bescherming van de vertrouwelijkheid van gegevens, temeer daar de risico's voortdurend evolueren.

103. De veiligheidsoefeningen en de opleiding over het ZNP zijn niet bedoeld om te voorzien in een opleiding over de beginselen van gegevensbescherming en -beveiliging. Tot slot vervangt de occasionele deelname van bepaalde werknemers aan de Cyber-Europe-dagen geen gestructureerde en voortgezette opleiding voor het volledige personeel. Het ziekenhuis toont geen proactieve en regelmatige aanpak aan wat betreft de opleiding/bewustmaking van zijn personeel inzake de specifieke vereisten van de AVG.

104. Tijdens de hoorzitting verklaarde de verweerder dat personeelsleden de mogelijkheid hebben om opleidingen te volgen over cybersecurity. Werknemers van het ziekenhuis hebben in oktober 2023 deelgenomen aan de cyberweek, waarvan het thema cybersecurity in de gezondheidszorg betrof. Hij rechtvaardigt ook de tussenkomst van een externe dienstverlener, die een twintigtal "AVG-kampioenen" heeft opgeleid. De Geschillenkamer neemt nota van deze inspanningen en bevestigt dat ze in de goede richting gaan, maar stelt vast dat deze opleidingen slechts betrekking hebben op een zeer klein deel van het personeel en pas na de gegevensinbreuk zijn ingevoerd.

105. **Bij wijze van conclusie kan worden gesteld dat het ziekenhuis niet beschikte over een echt opleidings-/bewustmakingsprogramma voor werknemers met betrekking tot de AVG en daarmee in strijd heeft gehandeld met de artikelen 32, 5.1.f) en 24 van de AVG.**

Over het systeem voor het bewaren van logbestanden met het oog op latere analyses bij incidenten

106. **De verweerder** beweert dat het ziekenhuis beschikt over een systeem voor het bewaren van logbestanden, dat vóór de gegevensinbreuk was ingevoerd. Hij geeft echter toe dat de aanvaller bewust een deel van deze logbestanden heeft verwijderd om sporen van zijn aanwezigheid uit te wissen. Tijdens de hoorzitting heeft de verweerder echter verklaard dat de logbestanden niet zijn verwijderd (in tegenstelling tot wat hij in zijn conclusie heeft betoogd), maar "versleuteld" door de aanvaller.

107. **De Geschillenkamer** herinnert aan de verplichting van de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen, met name het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen (artikel 32.1.b) van de AVG). Dit omvat ook het vermogen om logbestanden te bewaren met het oog op latere analyses bij gegevensinbreuken.

108. De Geschillenkamer stelt vast dat de verweerder de begrippen "het registeren van logbestanden" en "het bewaren van logbestanden" lijkt te verwarren. Het bewaren van logbestanden, waar het hier om gaat, heeft juist tot doel te voorkomen dat logbestanden worden verwijderd of versleuteld. Die bewaring is van cruciaal belang om achteraf te kunnen analyseren welke handelingen zijn uitgevoerd op de persoonsgegevens. In principe moet een dergelijk systeem voor het bewaren van logbestanden het mogelijk maken om gedurende een redelijke termijn vast te stellen wie toegang heeft gehad tot welke informatie, op welk moment en op welke wijze, en om de aard van de geraadpleegde informatie en de precieze identiteit van de persoon te achterhalen. Deze logbestanden moeten afzonderlijk worden bewaard op aparte

apparatuur, beveiligd tegen versleuteling, zodat een betrouwbare en veilige traceerbaarheid wordt gewaarborgd. De Geschillenkamer herinnert eraan dat de bovengenoemde minimale normen precieze en specifieke vereisten bevatten met betrekking tot het bewaren van logbestanden, die een goede praktijk vormen bij de implementatie van een dergelijk systeem.

109. In het onderhavige geval bevestigt de verweerder in zijn conclusie dat de aanvaller bewust een deel van deze logbestanden heeft verwijderd om de sporen van zijn aanwezigheid uit te wissen, met uitzondering van een server (radiologie) waar hij aanwijzingen heeft achtergelaten. Zonder bewaarde logbestanden is het moeilijk om de aanval te begrijpen, de misbruikte lekken te identificeren en de gecompromitteerde gegevens te beoordelen. De verweerder stelt dat de firewall-logbestanden tijdens de gegevensinbreuk niet zijn verwijderd, en dat de analyse daarvan erop wijst dat "waarschijnlijk acties en commando's door de aanvallers zijn geëxporteerd, en geen persoonsgegevens" (vrije vertaling). Omdat er geen logbestanden zijn bewaard, kan de verweerder dergelijke veronderstellingen echter onmogelijk aantonen.

110. Tijdens de hoorzitting betoogt de verweerder, in tegenspraak met deze conclusie, dat de logbestanden niet zijn "verwijderd", maar "versleuteld". Zelfs als de logbestanden zouden zijn versleuteld in plaats van verwijderd, toont de verweerder aan dat de logbestanden niet konden worden bewaard met het oog op latere analyses.

111. Deze situatie wijst op het ontbreken, of op zijn minst de ontoereikendheid, van het systeem voor het bewaren van logbestanden van het ziekenhuis ten tijde van de gegevensinbreuk (zie in dit verband de punten 19, 28 en 49 van de Richtsnoeren 01/2021 van de EDPB over voorbeelden betreffende de melding van inbreuken in verband met persoonsgegevens).

112. Tijdens de hoorzitting heeft de verweerder toegelicht dat de door het ziekenhuis aangebrachte verbeteringen in het back-upsysteem ervoor zorgen dat logbestanden niet langer verwijderd kunnen worden, en dat ze, mocht dat toch gebeuren, hersteld kunnen worden. De Geschillenkamer neemt kennis van deze technische maatregel, hoewel deze laat is doorgevoerd, zeker gezien het feit dat er al in 2019 een eerste gegevensinbreuk heeft plaatsgevonden.

113. **Bijgevolg heeft het ziekenhuis op het moment van de gegevensinbreuk de beveiligingsvereisten van de artikelen 5.1.f), 24 en 32 van de AVG geschonden door geen passende maatregelen te treffen om de logbestanden te beschermen tegen kwaadwillige verwijdering of versleuteling, waardoor het vermogen om gegevensinbreuken op te sporen en te analyseren met het oog op latere documentatie ervan in het gedrang kwam.**

Over systematische audits van de kwaliteit van de beveiliging van persoonsgegevens

114. **De verweerder** legt uit dat hij contractuele maatregelen heeft genomen om ervoor te zorgen dat verschillende dienstverleners de systemen van het ziekenhuis, de beveiliging en de kwaliteit van de gegevens auditen. Deze maatregelen zijn na de tweede gegevensinbreuk getroffen.

115. **De Geschillenkamer** herinnert eraan dat artikel 32.1.d) van de AVG een reeks technische en organisatorische maatregelen voorstelt, waaronder, indien nodig, een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen, teneinde de beveiliging van de verwerking te waarborgen.

116. Een audit van de kwaliteit van de gegevensbeveiliging maakt het mogelijk om de IT-infrastructuur te analyseren en de zwakke punten van de systemen voor het beheer van informatie (met inbegrip van persoonsgegevens) te identificeren, met name op het gebied van hardware, software, gegevens en procedures, teneinde een op het risico afgestemd beveiligingsniveau te waarborgen. Een gedetailleerd auditrapport stelt de verwerkingsverantwoordelijke in staat te weten welke kwetsbare zones blootgesteld zijn aan cybercriminelen. Op basis van een dergelijk rapport wordt een overzicht van de risico's opgesteld en worden passende beveiligingsmaatregelen aanbevolen om de geïdentificeerde risico's te beperken.

117. De minimale normen herinneren eraan dat elke organisatie "periodiek een conformiteitsaudit [moet] uitvoeren met betrekking tot de situatie rond informatieveiligheid en privacy zoals beschreven in de beleidslijnen", en dit minstens één keer per jaar. Uit het onderzoek van de Inspectiedienst is gebleken dat er op het moment van de inbreuk geen audit van de kwaliteit van de beveiliging van persoonsgegevens was uitgevoerd. Uit de door de verweerder verstrekte documenten blijkt dat er na de gegevensinbreuk verschillende audits zijn uitgevoerd.

118. Deze latere audits volstaan echter niet om aan te tonen dat het ziekenhuis vóór de tweede gegevensinbreuk het nodige heeft gedaan om gegevensinbreuken te voorkomen via systematische audits. Het ontbreken van dergelijke audits kan hebben bijgedragen aan het plaatsvinden van de tweede gegevensinbreuk, wat wijst op een tekortschietend proactief beheer van de beveiliging van persoonsgegevens. Bovendien verzoekt de Geschillenkamer het ziekenhuis om erop toe te zien dat de audits die na de tweede gegevensinbreuk zijn ingevoerd, voldoen aan de vereisten zoals uiteengezet in punt 116.

119. **Bij wijze van conclusie kan worden gesteld dat de verweerder zijn beveiligingsverplichting niet is nagekomen, doordat hij op het moment van de gegevensinbreuk geen regelmatige en systematische audits had ingevoerd om de**

doeltreffendheid van de technische en organisatorische maatregelen te testen, beoordelen en evalueren, en de beveiliging van de gegevensverwerkingen te waarborgen, zoals vereist door de artikelen 32, 24 en 5.1.f) van de AVG.

Over de beveiliging van het wachtwoord voor toegang tot het elektronische patiëntendossier

120. **De verweerder** is van oordeel dat hij beschikt over een sterke beveiliging van de wachtwoorden voor toegang tot de elektronische patiëntendossiers. Hij verklaart dit door het feit dat elke gebruiker, om toegang te krijgen tot de elektronische patiëntendossiers, toegang moet hebben tot de specifieke software van het ziekenhuis die lokaal op de computers en andere apparaten van het ziekenhuis is geïnstalleerd, en een toegangsaanvraagformulier moet invullen. Voor dit formulier is een gebruikersnaam nodig en moet de gebruiker een wachtwoord aanmaken. Ten tijde van de aanval moest dit wachtwoord tussen de 6 en 8 tekens bevatten en mocht het niet overeenkomen met de voornaam, achternaam, dienst of initialen van de gebruiker. Het ziekenhuis verklaart dat het voor het vaststellen van de wachtwoordcriteria afhankelijk is van de leverancier van zijn software voor het beheer van medische dossiers.

121. **De Geschillenkamer** herinnert eraan dat de AVG de verwerkingsverantwoordelijke verplicht om passende technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Deze maatregelen omvatten onder andere het vermogen om op permanente basis de vertrouwelijkheid van de verwerkingssystemen en diensten te garanderen (artikel 32.1b) van de AVG).

122. In een ziekenhuiscontext, waar de bescherming van gezondheidsgegevens van patiënten van cruciaal belang is, is een zeer sterk wachtwoord noodzakelijk. Aanbevelingen voor de beveiliging van wachtwoorden zijn te vinden in normen zoals die van het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA) en de richtsnoeren van het National Institute of Standards and Technology (NIST). Bovendien bepaalt de Nota informatieveiligheid en privacy: Synthese en vuistregels inzake de beveiliging van medische gegevens van 14 juli 2017, opgesteld op basis van besprekingen binnen de subwerkgroep "medische gegevens" van het Informatieveiligheidscomité[24], het volgende: "Een degelijk lang wachtwoord is minimaal 12 karakters lang." Een wachtwoord van 6 tot 8 tekens is echter zwak. Het biedt geen bescherming tegen *brute force*-aanvallen en vormt geen sterk authenticatiemiddel.

[24] Zie de categorie "Bijkomende documenten", en "NOTA MEDSEC Synthese en Vuistregels Beveiliging Medische Gegevens", beschikbaar via de volgende link: https://www.ksz-bcss.fgov.be/nl/gegevensbescherming/informatieveiligheidsbeleid#bijkomende-documenten.

123. De verweerder stelt in zijn conclusie dat het wachtwoordbeleid binnen het ziekenhuis is aangescherpt en dat wachtwoorden voortaan uit minimaal 8 tekens moeten bestaan. Op basis van de uiteenzettingen in het vorige punt acht de Geschillenkamer de lengte van een dergelijk wachtwoord echter ontoereikend op grond van de criteria van artikel 32.1 van de AVG, in het bijzonder rekening houdend met de stand van de techniek, de context en de risico's waarmee het ziekenhuis wordt geconfronteerd.

124. Hoewel de verweerder stelt dat elke gebruiker toegang moet hebben tot de specifieke software van het ziekenhuis en een toegangsaanvraagformulier moet invullen, om aan te tonen dat de beveiliging van wachtwoorden adequaat is, verzoekt de Geschillenkamer de verweerder om de invoering van tweefactorauthenticatie te overwegen. Deze technische maatregel wordt beschouwd als passend en proportioneel in verhouding tot de risico's. In de Richtsnoeren van de WP29 voor de melding van inbreuken in verband met persoonsgegevens[25] staat het volgende: "In de context van een ziekenhuis kan de onbeschikbaarheid van cruciale medische gegevens over patiënten, zelfs tijdelijk, een risico voor de rechten en vrijheden van natuurlijke personen inhouden. Het kan bijvoorbeeld tot gevolg hebben dat operaties worden geannuleerd en dat levens in gevaar komen."

125. Bovendien betekent het feit dat het ziekenhuis afhankelijk was van door zijn leverancier vastgestelde ontoereikende wachtwoordcriteria, dat het ziekenhuis een verwerker heeft ingeschakeld die ontoereikende waarborgen bood voor de uitvoering van passende technische en organisatorische maatregelen.

126. **Bij wijze van conclusie kan worden gesteld dat de verweerder geen rekening heeft gehouden met de criteria van de artikelen 32, 5.1.f) en 24 van de AVG om de sterkte van het wachtwoord aan te passen aan het beveiligingsniveau dat vereist is om de toegang tot de elektronische patiëntendossiers te beschermen.**

III. Sancties

III.1. Over de juridische kwalificatie van de verweerder

127. De Geschillenkamer heeft in haar analyse rekening gehouden met de antwoorden van de verweerder op het sanctieformulier en met de statuten van het ziekenhuis[26].

[25] Deze Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 zijn gepubliceerd door de WP29 (voorganger van de EDPB). Ze zijn beschikbaar via de volgende link: https://ec.europa.eu/newsroom/article29/items/612052/en (zie pagina 9).

[26] [...].

128. Artikel 221, § 2,[27] van de kaderwet bevat een uitzondering met betrekking tot het opleggen van een geldboete aan de "overheid" onder bepaalde voorwaarden. Het begrip "overheid" wordt gedefinieerd in artikel 5[28] van de kaderwet. De relevante criteria van artikel 5, 3°, van de kaderwet die door de verweerder zijn aangevoerd om aan te tonen dat hij als "overheid" moet worden gekwalificeerd, worden hieronder achtereenvolgens geanalyseerd.

129. Bij wijze van inleiding staat vast dat het ziekenhuis rechtspersoonlijkheid heeft als vereniging zonder winstoogmerk (hierna "vzw"), overeenkomstig de tweede voorwaarde van artikel 5, 3°, van de kaderwet.

Specifiek doel om te voorzien in behoeften van algemeen belang

130. De verweerder baseert zich voornamelijk op het maatschappelijk doel van het ziekenhuis, dat in de statuten is omschreven als "het verbeteren van het materiële en morele lot van de inwoners van (...)" (vrije vertaling), om aan te tonen dat het ziekenhuis voorziet in behoeften van algemeen belang, overeenkomstig de eerste voorwaarde van artikel 5, 3°, van de kaderwet.

131. Volgens de Geschillenkamer volstaat deze formulering, zoals die uit het maatschappelijk doel blijkt, echter niet om aan te tonen dat het ziekenhuis "specifiek" is opgericht om te voorzien in behoeften van algemeen belang, zoals vereist door artikel 5, 3°, van de kaderwet.

132. De rechtbanken hebben namelijk erkend dat ziekenhuizen op duurzame wijze een economisch doel nastreven, ook al is dat gewoonlijk ter ondersteuning van hun in principe altruïstische doelstellingen[29]. Het is dus duidelijk dat hun activiteit, hoewel die

---

[27] Artikel 221, § 2, van de kaderwet bepaalt het volgende: "Het artikel 83 van de Verordening is niet van toepassing op de overheid en hun aangestelden of gemachtigden, tenzij het gaat om een publiekrechtelijke rechtspersoon die goederen of diensten aanbiedt op een markt."

[28] Artikel 221, § 2, van de kaderwet bepaalt het volgende: "Het artikel 83 van de Verordening is niet van toepassing op de overheid en hun aangestelden of gemachtigden, tenzij het gaat om een publiekrechtelijke rechtspersoon die goederen of diensten aanbiedt op een markt."

[28] Artikel 5 van de kaderwet bepaalt het volgende: "Voor de toepassing van deze wet wordt verstaan onder “overheid” :

1° de Federale Staat, de deelstaten en lokale overheden;

2° de rechtspersonen van publiek recht die van de Federale Staat, de deelstaten of lokale overheden afhangen;

3° de personen, ongeacht hun vorm en aard, die :

- opgericht zijn met het specifieke doel te voorzien in behoeften van algemeen belang die niet van industriële of commerciële aard zijn; en

- rechtspersoonlijkheid hebben; en

- waarvan hetzij de activiteiten in hoofdzaak door de overheden of instellingen vermeld in de bepalingen onder 1° of 2°, worden gefinancierd, hetzij het beheer onderworpen is aan toezicht door deze overheden of instellingen, hetzij de leden van het bestuursorgaan, leidinggevend orgaan of toezichthoudend orgaan voor meer dan de helft door deze overheden of instellingen zijn aangewezen;

4° de verenigingen bestaande uit één of meer overheden als bedoeld in de bepalingen onder 1°, 2° of 3°."

[29] Zie in dit verband de zaak voor de burgerlijke rechtbank Oost-Vlaanderen (afdeling Gent) (2e kamer) van 27 april 2015, waarin wordt herinnerd aan het feit dat actoren uit de zogenaamde "socialprofitsector", zoals ziekenhuizen, meestal onder het begrip "onderneming" vallen, aangezien zij op duurzame wijze een economisch doel nastreven, ook al is dat meestal ter ondersteuning

onder een altruïstisch kader valt, deel uitmaakt van een aanpak waarin financiële levensvatbaarheid en het streven naar economische efficiëntie belangrijke componenten zijn, zelfs als het ziekenhuis is opgericht in de vorm van een vzw. Bijgevolg is de oprichting van deze entiteiten niet uitsluitend gericht op het voorzien in behoeften van algemeen belang, maar houdt zij ook rekening met economische overwegingen die niet mogen worden genegeerd bij de beoordeling van hun juridische kwalificatie in de zin van artikel 5, 3°, van de kaderwet.

133. Het ziekenhuis is niet "specifiek" opgericht om te voorzien in behoeften van algemeen belang, maar volgt een eigen economische logica, zodat niet is voldaan aan de eerste voorwaarde van artikel 5, 3°, van de kaderwet.

Financiering van het ziekenhuis:

134. In zijn antwoord op het sanctieformulier heeft de verweerder de inkomsten van het ziekenhuis gedetailleerd uiteengezet aan de hand van vijf belangrijke inkomstenbronnen, die volgens hem bijna allemaal door de overheid worden gefinancierd, zodat aan de laatste voorwaarde van artikel 5, 3°, van de kaderwet zou zijn voldaan.

135. Drie van de vijf inkomstenbronnen zijn afkomstig van de overheid. Twee financieringsbronnen behoeven echter een gedetailleerde analyse. Deze vertegenwoordigen, op basis van de door de verweerder gerapporteerde cijfers[30], het grootste deel van de financiering van het ziekenhuis. Volgens de door de verweerder verstrekte cijfers is bijna de helft (..%) van zijn inkomsten afkomstig van de "honoraria van artsen", en (..%) van de "verkoop van farmaceutische producten" (vrije vertaling).

136. De verweerder stelt het volgende:

    a. De honoraria van artsen, die voornamelijk aan het RIZIV[31] worden gefactureerd via de verzekeringsinstellingen (ziekenfondsen en HZIV[32]), bestaan uit de facturering van prestaties en therapeutische handelingen van zorgverleners aan de sociale zekerheid.

    b. De inkomsten uit de verkoop van farmaceutische producten vloeien voort uit de facturering van geneesmiddelen, voornamelijk aan het RIZIV via de

van hun in principe altruïstische doelstellingen. In deze zaak vormde het feit dat de eiser de vorm had van een vereniging zonder winstoogmerk geen belemmering. Hij werd als onderneming beschouwd, ondanks het feit dat hij geen winstoogmerk had.

[30] De inkomsten van 2021 en 2023 werden verstrekt door de verweerder. De Geschillenkamer baseerde zich op de cijfers uit 2023, ook al zou de analyse met de cijfers uit het boekjaar 2021 grotendeels hetzelfde zijn geweest.

[31] Het RIZIV is het Rijksinstituut voor ziekte- en invaliditeitsverzekering. Het is een federale instelling.

[32] Indien een verzekerde niet bij een ziekenfonds is aangesloten, treedt de Hulpkas voor Ziekte- en Invaliditeitsverzekering (HZIV), een openbare instelling van sociale zekerheid, op in het kader van de verplichte verzekering. Zij vertegenwoordigt 100 000 leden of 1 % van de markt. Deze financieringsbron is publiek, wat niet wordt betwist door de Geschillenkamer.

verzekeringsinstellingen (ziekenfondsen en HZIV) en aan de patiënten, in voorkomend geval in de vorm van forfaitaire bedragen.

137. De verweerder stelt ook het volgende (vrije vertaling): "Hoewel de ziekenfondsen rechtspersonen van publiek recht zijn, worden zij in hoofdzaak gefinancierd door het RIZIV, een rechtspersoon van publiek recht die van de Federale Staat afhangt, via de verplichte verzekering die in hoofdzaak tussenkomt." De verweerder is dan ook van oordeel dat de financieringsbron van het ziekenhuis in hoofdzaak publiek is, aangezien deze afkomstig is van het RIZIV, zodat het ziekenhuis als overheid moet worden gekwalificeerd.

138. De Geschillenkamer volgt deze redenering niet. Het RIZIV is weliswaar een overheidsinstelling, maar zijn rol beperkt zich tot het terugbetalen van een deel van de zorg die aan patiënten wordt verleend in het kader van de verplichte ziekteverzekering. Dit mechanisme houdt geen rechtstreekse financiering van ziekenhuizen in, maar maakt deel uit van een complex systeem waarin elke burger verplicht is een ziekteverzekering af te sluiten om recht te hebben op een bijdrage van de Staat in zijn kosten, in het kader van de sociale zekerheid. Dankzij de derdebetalersregeling kunnen patiënten behandeld worden zonder de volledige kosten te moeten voorschieten, maar dit betekent niet dat het ziekenhuis zelf rechtstreeks door het RIZIV wordt gefinancierd.

139. Dit unieke terugbetalingssysteem verschilt fundamenteel van het financieringsconcept zoals bedoeld in artikel 5, 3°, van de kaderwet. Het ziekenhuis wordt dus niet in hoofdzaak gefinancierd door de overheid of de instellingen vermeld in artikel 5, 1° of 2°, van de kaderwet. Aan de laatste voorwaarde van artikel 5, 3°, van de kaderwet betreffende overwegende financiering door de overheid is niet voldaan.

Het beheer is onderworpen aan toezicht door de overheid:

140. Volgens de verweerder wordt het Belgische ziekenhuiswezen georganiseerd door de overheid. Hij stelt dat het Waals Agentschap voor Levenskwaliteit ("AVIQ") de Waalse gewestelijke overheidsdienst is die belast is met het beheer van de erkenning van gewestelijke ziekenhuizen en de inspectie daarvan. Bijgevolg is het beheer van het ziekenhuis volgens de verweerder onderworpen aan toezicht door de overheid. Bovendien is hij van oordeel dat de overheid zowel toezicht houdt op de inkomsten (de door ziekenhuizen gehanteerde tarieven) als op de uitgaven.

141. De Geschillenkamer verwerpt opnieuw de argumenten van de verweerder en maakt daarbij een duidelijk onderscheid tussen de begrippen regelgeving en effectief toezicht op het beheer. Het Waals Agentschap voor Levenskwaliteit ("AVIQ") heeft weliswaar een inspectie- en erkenningsopdracht, maar deze taken vallen uitsluitend onder het regelgevend toezicht dat tot doel heeft de naleving van specifieke normen

op het gebied van de kwaliteit van de zorg te waarborgen. Deze externe controlemechanismen zijn weliswaar noodzakelijk om de veiligheid en de kwaliteit te waarborgen, maar mogen niet worden verward met rechtstreeks toezicht op het interne beheer van de ziekenhuizen door de overheid.

142. Het beheer van het ziekenhuis, als vzw, is onderworpen aan het Wetboek van vennootschappen en verenigingen, dat de interne activiteiten ervan regelt zoals die van elke andere private entiteit. De besluitvormingsorganen van het ziekenhuis, namelijk de raad van bestuur en de algemene vergadering, bestaan uitsluitend uit particulieren, zoals bepaald in de artikelen 6, 7 en 11 van de statuten van de vereniging. Er is geen enkele statutaire of wettelijke bepaling die de aanwezigheid van vertegenwoordigers van de overheid in deze organen voorschrijft. Bovendien worden beslissingen over de financiële strategie, de aanwerving van personeel of het beheer van de infrastructuur genomen zonder inmenging van de overheid.

143. Het wettelijk kader legt ziekenhuizen bepaalde verplichtingen op wat betreft tarieven en uitgaven, maar het gaat hier niet om rechtstreeks financieel toezicht. De overheid beslist niet over de toewijzing van middelen of het beheer van ziekenhuisbudgetten. Deze vallen onder de bevoegdheid van de interne beheersorganen van het ziekenhuis, die hun beslissingsautonomie en eigen verantwoordelijkheid op het gebied van financieel beheer behouden. Bovendien kan de algemene vergadering van het ziekenhuis, zonder inmenging van de overheid, besluiten het ziekenhuis te ontbinden (artikel 39 van de statuten).

144. Ten slotte blijkt uit de parlementaire debatten over de kaderwet dat de wetgever nooit heeft beoogd om ziekenhuizen in de vorm van een vzw uit te sluiten van de regeling inzake administratieve geldboeten waarin de AVG en de kaderwet voorzien. Zelfs in gevallen die complexer zijn dan de onderhavige zaak, waarin een ziekenhuis wordt beheerd door een Openbaar Centrum voor Maatschappelijk Welzijn ("OCMW"), waren de parlementsleden van oordeel dat een dergelijk ziekenhuis onderworpen moest zijn aan de regeling inzake administratieve geldboeten: "Organisaties die in essentie dezelfde activiteiten uitoefenen moeten op dezelfde wijze behandeld worden, onafhankelijk of zij nu tot de publieke of de private sector behoren. Zo valt het bijvoorbeeld niet te verantwoorden dat een OCMW-ziekenhuis geen administratieve boete kan worden opgelegd terwijl dit wel zou kunnen voor een ziekenhuis in de vorm van een vzw (...)."[33] (onderstreept door de Autoriteit)

[33] Verslag namens de Commissie voor de Justitie uitgebracht door de heer P. Dedecker, Parlementaire stukken Kamer 2017-2018, nr. 54-3126/3, p. 44, beschikbaar via de volgende link: https://www.dekamer.be/FLWB/PDF/54/3126/54K3126003.pdf.

145. Het ziekenhuis blijft dus, hoewel het onderworpen is aan regelgeving en inspecties, een autonome entiteit waarvan het beheer niet kan worden gelijkgesteld met toezicht door de overheid zoals bedoeld in artikel 5 van de kaderwet. Aan de laatste voorwaarde van artikel 5, 3°, van de kaderwet betreffende het beheer door de overheid is niet voldaan. Bij wijze van conclusie zal de Geschillenkamer de kwalificatie van Y als een privaatrechtelijke vzw handhaven, zonder dat er een band van ondergeschiktheid of mandaat bestaat tussen het ziekenhuis en enige overheidsinstantie. Deze kwalificatie verhindert dat het ziekenhuis aanspraak kan maken op de uitzondering van artikel 221, § 2, van de kaderwet, wat betreft het opleggen van een geldboete op basis van artikel 83 van de AVG.

146. Om alle verwarring dienaangaande te vermijden, stemt de verweerder ermee in dat artikel 221, § 2, van de kaderwet – dat bepaalt dat publiekrechtelijke rechtspersonen die goederen en/of diensten op een markt aanbieden, niet zijn vrijgesteld van de administratieve geldboete – in het kader van de onderhavige procedure niet moet worden onderzocht. Hij betwist namelijk niet dat het ziekenhuis een privaatrechtelijke rechtspersoon is.

III.2. Over de geldboete

147. De Geschillenkamer heeft in haar analyse rekening gehouden met de antwoorden van de verweerder op het sanctieformulier.

III.2.1. Herinnering aan de toepasselijke wettelijke bepalingen

148. Als onafhankelijke administratieve autoriteit heeft de Geschillenkamer de exclusieve bevoegdheid om passende corrigerende maatregelen en sancties vast te stellen overeenkomstig de relevante bepalingen van de AVG en de WOG. Deze bevoegdheid vloeit specifiek voort uit de artikelen 58 en 83 van de AVG, zoals bevestigd door de rechtspraak van het Marktenhof in zijn arresten van 7 juli 2021, 19 februari 2020 en 20 december 2023[34], waarin de omvang van de discretionaire bevoegdheid van de Geschillenkamer met betrekking tot de keuze van sancties en de hoogte van de geldboete werd benadrukt.

149. Volgens de richtsnoeren van de EDPB en de AVG heeft de toezichthoudende autoriteit de discretionaire bevoegdheid om een geldboete op te leggen[35]. De AVG

[34] Marktenhof, 19de kamer A, arrest van 7 juli 2021, 2021/AR/320 (hier beschikbaar), p. 37-47; Marktenhof, 19de kamer A, arrest van 19 februari 2020, 2020/AR/1160, (hier beschikbaar) p. 30-31; Marktenhof, 19de kamer A, arrest van 20 december 2023, 2023/AR/817, (hier beschikbaar) p. 57, 61 en 62.

[35] EDPB – Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG, vastgesteld op 24 mei 2023 (v2.1), beschikbaar op de website: https://www.edpb.europa.eu/system/files/2024-

verplicht elke toezichthoudende autoriteit ervoor te zorgen dat de administratieve geldboeten die worden opgelegd, in elke zaak doeltreffend, evenredig en afschrikkend zijn (artikel 83.1 van de AVG).

150. Bovendien moet de toezichthoudende autoriteit bij het vaststellen van de hoogte van de geldboete voor elk concreet geval naar behoren rekening houden met verschillende specifieke elementen, zoals "*de aard, de ernst en de duur van de inbreuk, rekening houdend met de aard, de omvang of het doel van de verwerking in kwestie alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade*" (artikel 83.2.a) van de AVG); "*de opzettelijke of nalatige aard van de inbreuk*" (artikel 83.2.b) van de AVG); en "*de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft*" (artikel 83.2.g) van de AVG).

151. Bijgevolg moet elke geldboete[36] worden beoordeeld rekening houdend met alle factoren die worden genoemd in artikel 83.2.a)–k) van de AVG, zonder echter het wettelijk vastgestelde maximumbedrag van artikel 83.4–6 van de AVG te overschrijden.

152. Overeenkomstig overweging 148 van de AVG dienen straffen, met inbegrip van administratieve geldboeten, te worden opgelegd naast of in plaats van passende maatregelen in geval van een ernstige schending, zelfs wanneer het de eerste vaststelling van een schending betreft[37]. Het feit dat strafbaar gedrag slechts voor het eerst bij een verweerder wordt vastgesteld, belet de Geschillenkamer dus niet om een administratieve geldboete op te leggen overeenkomstig artikel 58.2.i) van de AVG.

III.2.2. Redenen voor het opleggen van een geldboete

153. Het HvJ-EU heeft onlangs geoordeeld dat wanneer de vaststelling van een inbreuk in verband met persoonsgegevens plaatsvindt, de toezichthoudende autoriteit niet verplicht is om een corrigerende maatregel te nemen, in het bijzonder een administratieve geldboete, op grond van artikel 58.2 van de AVG, wanneer een dergelijke maatregel niet passend, noodzakelijk of evenredig is om de vastgestelde tekortkoming te verhelpen en de volledige naleving van deze verordening te waarborgen[38].

01/edpb_guidelines_042022_calculationofadministrativefines_nl_0.pdf, zie punten 15, 20, 69, 84, 144; AVG, overwegingen 148, 150; artikel 58.1.i) en artikel 83.

[36] HvJ-EU, arrest van 5 december 2023, Deutsche Wohnen SE tegen Staatsanwaltschaft Berlin, C-807/21, EU:C:2023:950; HvJ-EU, arrest van 5 december 2023, Nacionalinis visuomenės sveikatos centras, C-683/21, ECLI:EU:C:2023:949.

[37] HvJ-EU, 5 december 2023, C-807/21, *Deutsche Wohnen SE t. Staatsanwaltschaft Berlin* (ECLI:EU:C:2023:950), punt 38.

[38] Arrest van het HvJ-EU, C-768/21, van 26 september 2024, ECLI:EU:C:2024:785.

154. De Geschillenkamer besluit een administratieve geldboete op te leggen omdat zij van oordeel is dat, gezien de specifieke omstandigheden van de zaak zoals hieronder uiteengezet en rekening houdend met de relevante criteria van artikel 83.2 van de AVG, een geldboete passend is. De bovengenoemde relevante criteria gelden dus niet alleen bij het opleggen van een geldboete overeenkomstig artikel 83.1 van de AVG, maar ook bij de keuze tussen de verschillende soorten sancties die zijn voorzien in artikel 58.2 van de AVG en artikel 100 van de WOG[39].

155. Om te beslissen dat een administratieve geldboete in het onderhavige geval passend was, hanteert de Geschillenkamer de volgende criteria[40]:

- **De ernst van de inbreuken:** gezien de gevoelige aard van de gegevens die in deze ziekenhuiscontext worden verwerkt, zijn de vastgestelde inbreuken bijzonder ernstig. Gezondheidsgegevens genieten vanwege hun gevoelige aard een versterkte bescherming en vereisen "betere" bescherming[41]. Ziekenhuizen zijn bijzonder kwetsbaar voor gegevensinbreuken. Hoewel sommige van deze inbreuken ondanks de invoering van passende technische en organisatorische maatregelen onvermijdelijk zijn, kunnen andere worden voorkomen. Om ze te voorkomen, voorziet de AVG in de afstemming van deze beveiligingsmaatregelen op het risico dat de verwerking met zich meebrengt, alsook in de invoering van een GEB om de risico's vooraf beter te beheren en de passende maatregelen te bepalen. Het is duidelijk dat de technische en organisatorische maatregelen die bij de gegevensinbreuk in 2021 van kracht waren, ontoereikend waren en niet voldeden aan de wettelijke verplichtingen, met name die welke zijn opgelegd door artikel 32 van de AVG. Deze schending is des te ernstiger omdat zij zich voordoet na een eerder geval van dezelfde aard (ransomware). Deze omstandigheid had het ziekenhuis ertoe moeten aanzetten zijn risico's opnieuw te evalueren en zijn beveiligingsmaatregelen op passende wijze te versterken, onder meer door een GEB uit te voeren. Het feit dat een ziekenhuis, dat verantwoordelijk is voor de verwerking van persoonsgegevens van 300 000 patiënten, niet alle nodige maatregelen heeft getroffen om een tweede gegevensinbreuk te voorkomen, vormt een fout die de meest afschrikkende sanctie rechtvaardigt.

- **De duur van de inbreuk**: de passende technische en organisatorische maatregelen om een nieuwe soortgelijke gegevensinbreuk te voorkomen, hadden uiterlijk na de eerste gegevensinbreuk moeten worden genomen. De Geschillenkamer merkt echter op dat veel beveiligingsmaatregelen pas na de tweede gegevensinbreuk werden ingevoerd, dat wil

---

[39] Wat betreft de voorwaarden om te beoordelen of het opleggen van een geldboete opportuun is, merkt de Geschillenkamer op dat deze voorwaarden uitvoerig zijn vastgelegd in de Richtsnoeren voor de toepassing en vaststelling van administratieve geldboeten in de zin van Verordening (EU) 2016/679, goedgekeurd op 3 oktober 2019 door de werkgroep WP29, beschikbaar via de volgende link: https://ec.europa.eu/newsroom/article29/items/611237/en.

[40] Marktenhof, 19de kamer A, arrest van 19 februari 2020, 2020/AR/1160, p. 30-31; deze criteria kunnen ook worden gebruikt om het bedrag van de geldboete te beoordelen, overeenkomstig de bovengenoemde richtsnoeren van 3 oktober 2019.

[41] Zie artikel 9 en overweging 55 van de AVG.

zeggen 2 jaar en 6 maanden na deze gebeurtenis, en dat deze invoering onvolledig was. Gezien de risico's waarmee ziekenhuizen worden geconfronteerd en het hogere beschermingsniveau dat aan gezondheidsgegevens wordt toegekend, kunnen ziekenhuizen niet rekenen op een grote flexibiliteit wat betreft de termijnen voor de implementatie van hun beveiligings- en risicopreventiemaatregelen. Het ziekenhuis heeft de dringende noodzaak om al zijn beveiligingsmaatregelen in overeenstemming te brengen met de geldende regelgeving niet onderkend, zelfs niet na de eerste gegevensinbreuk in 2019. Deze termijn rechtvaardigt een passende reactie van de Geschillenkamer.

- **Het afschrikkende effect dat nodig is om toekomstige inbreuken te voorkomen**: de Geschillenkamer acht het betreurenswaardig dat het ziekenhuis niet vooraf de nodige technische en organisatorische maatregelen heeft getroffen om een tweede gegevensinbreuk te voorkomen. Een eenvoudige waarschuwing zou een onvoldoende afschrikkend effect hebben, wat toezichthoudende autoriteiten in aanmerking moeten nemen bij het bepalen van een passende sanctie. Een louter bevel tot naleving zou ertoe kunnen leiden dat het ziekenhuis – en bij uitbreiding andere Belgische ziekenhuizen – de vaststelling van dergelijke inbreuken door de Geschillenkamer beschouwen als het startpunt van hun inspanningen om aan de voorschriften te voldoen. Dit zou de beveiligingsvereisten van de AVG ernstig ondermijnen. Door te kiezen voor een geldboete benadrukt de Geschillenkamer de ernst van deze inbreuken en de noodzaak van een grotere zorgvuldigheid bij de beveiliging van persoonsgegevens in ziekenhuizen. Zij wenst in het bijzonder aan te tonen dat gegevensinbreuken die voortvloeien uit ernstige en aanhoudende nalatigheid op het gebied van risicobeheer, kunnen leiden tot strenge sancties.

156. Gezien de context die uit een dergelijke beoordeling naar voren komt, heeft de Geschillenkamer bepaald dat een administratieve geldboete een passende sanctie is om een krachtig signaal te geven, niet alleen aan de verweerder, maar ook aan alle Belgische ziekenhuizen. Deze sanctie bewijst dat niet-naleving van de AVG-vereisten tot strenge sancties leidt wanneer de ernst van de inbreuk dit rechtvaardigt, zoals in het onderhavige geval.

III.2.3. Uitgangsbedrag voor de berekening van de administratieve geldboete

157. Om in elk geval een geldboete op te leggen die doeltreffend, evenredig en afschrikkend is, dienen toezichthoudende autoriteiten administratieve geldboeten aan te passen binnen het bereik zoals voorzien in de richtsnoeren van de EDPB[42], tot

[42] EDPB – Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG, vastgesteld op 24 mei 2023 (v2.1), zie punten 21 tot en met 45.

aan het wettelijke maximumbedrag. Dit kan leiden tot aanzienlijke verhogingen of verlagingen van het bedrag van de geldboete, afhankelijk van de omstandigheden van het geval.

i. Classificatie op basis van de inbreuken overeenkomstig artikel 83, leden 4 en 5, van de AVG[43]

158. De AVG maakt een onderscheid tussen twee categorieën van inbreuken: enerzijds de inbreuken die strafbaar zijn op grond van artikel 83.4 van de AVG, en anderzijds de inbreuken die strafbaar zijn op grond van artikel 83.5 en artikel 83.6 van de AVG. De eerste categorie van inbreuken leidt tot een geldboete van maximaal 10 miljoen EUR of, voor een onderneming, 2 % van de jaaromzet, indien dit cijfer hoger is. De tweede categorie kan leiden tot een geldboete van maximaal 20 miljoen EUR of, voor een onderneming, 4 % van de jaaromzet, indien dit cijfer hoger is.

159. In het onderhavige geval stelt de Geschillenkamer een inbreuk op verschillende artikelen vast, namelijk de volgende:

- artikel 35.3 van de AVG, betreffende de gegevensbeschermingseffectbeoordeling;
- artikel 32 van de AVG, betreffende de beveiliging van de verwerking;
- artikel 5.1.f) van de AVG, betreffende het beginsel van integriteit en vertrouwelijkheid;
- artikel 24 van de AVG, betreffende de verantwoordelijkheid van de verwerkingsverantwoordelijke.

160. De hoogste boete is van toepassing, overeenkomstig artikel 83.5.b) van de AVG. In geval van een inbreuk op artikel 5 (in dit geval het beginsel van integriteit en vertrouwelijkheid) kan de Geschillenkamer een administratieve geldboete opleggen tot 20.000.000 EUR of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

161. **In het onderhavige geval blijkt dat de omzet van de verweerder voor het jaar 2023, dat voorafgaat aan het jaar waarin de beslissing in deze zaak zal worden genomen en dus het referentieboekjaar vormt, is vastgesteld op (.. EUR). Op basis hiervan bedraagt de maximale boete 20.000.000 EUR.**

ii. Ernst van de inbreuk in elk afzonderlijk geval

[43] EDPB – Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG, vastgesteld op 24 mei 2023 (v2.1), beschikbaar op: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_nl, zie punten 49 en 50.

162. De hieronder uiteengezette criteria volgen de methode die is vastgelegd in de richtsnoeren voor de berekening van geldboeten van de EDPB[44]. De Geschillenkamer herinnert eraan dat zij niet verplicht is om criteria te onderzoeken die niet van toepassing zijn[45].

Aard, ernst en duur van de inbreuk (artikel 83.2.a) van de AVG)

163. *Ten eerste*, wat betreft de aard van de inbreuken in deze zaak, gaat het om een reeks schendingen van verschillende artikelen van de AVG:

- **Artikel 35.3 van de AVG**: het ontbreken van een GEB heeft het ziekenhuis de mogelijkheid ontnomen om zijn informaticasystemen beter in kaart te brengen en zodoende na te denken over passende maatregelen om risico's, met name het risico op gegevensinbreuken, het hoofd te bieden.
- **Artikel 32 van de AVG**: het gebrek aan passende technische en organisatorische maatregelen vergroot het risico op gegevensinbreuken en vermindert het vermogen van de verwerkingsverantwoordelijke om deze te documenteren, waardoor de bescherming van persoonsgegevens tegen ongeoorloofde toegang in het gedrang komt.
- **Artikel 5.1.f) van de AVG**: ontoereikende beveiligingsmaatregelen ondermijnen het beginsel van integriteit en vertrouwelijkheid doordat gegevens kwetsbaar worden gemaakt voor ongeoorloofde toegang, wijziging en openbaarmaking. Dit doet rechtstreeks afbreuk aan de toepassing van artikel 5.1.f) van de AVG, dat beoogt te waarborgen dat persoonsgegevens op een veilige manier worden verwerkt.
- **Artikel 24 van de AVG**: ontoereikende beveiligingsmaatregelen, waaronder het uitblijven van regelmatige bijwerkingen, wijzen op een tekortkoming van de verwerkingsverantwoordelijke bij het nakomen van de verplichtingen uit hoofde van artikel 24 van de AVG, dat vereist dat passende maatregelen worden geïmplementeerd en continu geactualiseerd om de naleving van de AVG te waarborgen en aan te tonen.

164. *Ten tweede*, wat betreft de ernst van de inbreuk, houdt de Geschillenkamer rekening met de volgende elementen:

- **Aard van de verwerking**: in een ziekenhuiscontext worden op grote schaal gevoelige gegevens van kwetsbare personen beheerd, waarbij bijzondere aandacht moet worden besteed aan beveiligingsmaatregelen om de risico's voor betrokkenen te beperken. De EDPB benadrukt in zijn richtsnoeren dat gevallen van ransomware aanzienlijke risico's

[44] EDPB – Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG, vastgesteld op 24 mei 2023 (v2.1), beschikbaar op: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_nl, zie punt 17.

[45] EDPB – Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG, vastgesteld op 24 mei 2023 (v2.1), beschikbaar op: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_nl, zie punt 6.

inhouden[46], en verwijst daarbij naar het voorbeeld van een ziekenhuis dat slachtoffer werd van een ransomware-aanval waardoor gegevens gedurende twee dagen onbeschikbaar waren.

- **Doeleinde van de verwerking in het kader van de hoofdactiviteiten**: de verwerkingen die het voorwerp van het onderzoek uitmaakten, betreffen het beheer van de informaticasystemen van de verweerder, in het bijzonder de mailboxen van het personeel en de medische dossiers, die essentieel zijn voor de beveiliging van de gegevens van de patiënten en dus voor de continuïteit van de zorg.
- **Aantal betrokkenen**: het ziekenhuis telt 300 000 patiënten in zijn databank, wat geldt als referentieaantal voor de personen die door de inbreuk zijn getroffen. Aangezien de patiëntgegevens tijdelijk onbeschikbaar waren, ook via de software die de medische dossiers ondersteunt, maken de gezondheidsgegevens van deze 300 000 patiënten van het ziekenhuis deel uit van de gegevensinbreuk[47]. Daarnaast zijn deze 300 000 personen ook betrokken bij de door de Inspectiedienst vastgestelde schendingen, met name wat betreft de beveiliging van het wachtwoord voor toegang tot hun elektronische medische dossiers. Ook de werknemers van het ziekenhuis zijn getroffen door de gegevensinbreuk, aangezien zij tijdelijk geen toegang hadden tot hun mailboxen en tot de elektronische patiëntendossiers, die hun voornaamste werkinstrumenten vormen.
- **Omvang van de schade**[48]: de Geschillenkamer oordeelt dat de ontoereikendheid van de technische en organisatorische maatregelen van de verweerder heeft bijgedragen aan het mogelijk maken van de gegevensinbreuk van 2021. De continuïteit van de patiëntenzorg op de spoedeisende hulp werd gedurende drie dagen verstoord, waardoor dringend zorgbehoevende patiënten moesten worden doorverwezen naar andere ziekenhuizen. Door deze gegevensinbreuk had het personeel ook meer dan een week geen toegang tot hun e-mail en duurde het enkele dagen voordat de software voor toegang tot de patiëntendossiers weer (voor 95 %) operationeel was, wat de continuïteit van de zorg verstoorde doordat de apparatuur die nodig is voor de goede werking van het ziekenhuis niet beschikbaar was. De omvang van de schade wordt dan ook als matig beschouwd.

165. *Ten derde*, wat betreft de duur van de inbreuk, wijst de Geschillenkamer erop dat deze niet ziet op de duur van de gegevensinbreuk zelf, noch op de schadelijke

[47] EDPB – Richtsnoeren 01/2021 over voorbeelden betreffende de melding van inbreuken in verband met persoonsgegevens (v2), vastgesteld op 14 december 2021 en beschikbaar via de volgende link: https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_nl.pdf. Wat betreft de tijdelijke onbeschikbaarheid van gegevens als een vorm van gegevensinbreuk (vrije vertaling): "*Bijgevolg wordt een beveiligingsincident dat leidt tot de tijdelijke onbeschikbaarheid van persoonsgegevens ook beschouwd als een vorm van inbreuk, aangezien het verlies van toegang tot de gegevens een aanzienlijke invloed kan hebben op de rechten en vrijheden van natuurlijke personen.*" (pagina 9)

[48] Overeenkomstig overweging 75 van de AVG verwijst de omvang van de schade naar ernstige lichamelijke, materiële of immateriële schade.

gevolgen daarvan, zoals beschreven in het vorige punt. De technische en organisatorische maatregelen van het ziekenhuis hadden immers al sinds de inwerkingtreding van de AVG op 25 mei 2018, en op zijn minst sinds de eerste gegevensinbreuk op [datum] 2019, getroffen moeten zijn. De duur van de inbreuk wordt dan ook berekend vanaf deze laatste gebeurtenis tot aan de gegevensinbreuk van september 2021, die het begin markeert van de inspanningen om de beveiligingsmaatregelen in overeenstemming te brengen. Dit komt neer op een periode van 2 jaar en 6 maanden. Deze duur wordt als matig beschouwd.

Opzettelijke of nalatige aard van de inbreuk (artikel 83.2.b) van de AVG)

166. Er wordt een onderscheid gemaakt tussen een door nalatigheid veroorzaakte inbreuk en een opzettelijk veroorzaakte inbreuk. De opzettelijke aard van een inbreuk impliceert dat aan twee voorwaarden wordt voldaan, namelijk kennis van de inbreuk en de wil om deze te plegen. Nalatigheid wordt daarentegen gekenmerkt door het ontbreken van opzet bij het plegen van de inbreuk, hoewel het zorgvuldigheidsbeginsel niet werd gerespecteerd.

167. De Geschillenkamer wijst erop dat er een hoge drempel is om een inbreuk als opzettelijk aan te merken. Verder kan nalatigheid ook in gradaties worden beoordeeld.

168. In het onderhavige geval blijkt geen opzet uit de schendingen. Aangezien de verwerking van gevoelige gegevens echter de kernactiviteit van de verweerder is en de verweerder al eerder te maken heeft gehad met een gegevensinbreuk, is de Geschillenkamer van oordeel dat de verweerder ernstig nalatig is geweest. Dit criterium versterkt de ernst van de inbreuk.

Categorieën van persoonsgegevens waarop de inbreuk betrekking heeft (artikel 83.2.g) van de AVG)

169. Uit de stukken van het dossier blijkt dat de inbreuk betrekking heeft op gevoelige gegevens die onder de beschermingsregeling van artikel 9 van de AVG vallen, met name gezondheidsgegevens. De inbreuk op deze categorieën van gegevens versterkt de ernst van de inbreuk.

Classificatie van de ernst van de inbreuk en vaststelling van het passende uitgangsbedrag

170. Op basis van de beoordeling van de bovenstaande elementen – namelijk de aard, ernst en duur van de inbreuk, alsmede de opzettelijke of nalatige aard van de inbreuk en de categorieën van persoonsgegevens in kwestie – kan de ernst van de inbreuk in haar

geheel worden bepaald. Op basis van deze beoordeling kan de ernst van de inbreuk worden gekwalificeerd als "laag", "gemiddeld" of "hoog".

171. In het onderhavige geval moet in de eerste plaats worden opgemerkt dat de inbreuk op artikel 5 van de AVG voorkomt in de lijst van inbreuken in artikel 83.5 van de AVG en dus onder het hoogste niveau van artikel 83 van die verordening valt.

172. De betrokken verwerkingen van gevoelige gegevens hebben betrekking op het beheer van de medische dossiers van kwetsbare personen (patiënten) en de mailboxen van het ziekenhuispersoneel, die essentieel zijn voor de continuïteit van de zorg. Bovendien blijkt dat 300 000 patiënten in de databanken van het ziekenhuis zijn opgenomen en dat ook de werknemers van het ziekenhuis door de gegevensinbreuk zijn getroffen.

173. De vastgestelde schade blijft echter relatief beperkt, met als belangrijkste gevolgen dat de mailboxen van het personeel gedurende 12 dagen niet beschikbaar waren, de elektronische medische dossiers gedurende 3 dagen niet beschikbaar waren en de spoedeisende hulp gedurende 3 dagen verstoord was.

174. In ieder geval is de inbreuk door de verweerder het gevolg van ernstige nalatigheid van zijn kant, temeer daar het ziekenhuis in 2019 al een eerste gegevensinbreuk heeft meegemaakt. De meeste beveiligingsmaatregelen die na de tweede gegevensinbreuk zijn genomen, hadden al sinds de inwerkingtreding van de AVG moeten zijn getroffen.

175. In het licht van het bovenstaande concludeert de Geschillenkamer dat de vastgestelde inbreuk van gemiddelde ernst is. Voor de berekening van het bedrag van de geldboete zal daarom een uitgangsbedrag worden vastgesteld tussen 10 % en 20 % van het wettelijke maximumbedrag van 20 000 000 EUR zoals bepaald in artikel 83.5 van de AVG[49], dat wil zeggen tussen 2 000 000 en 4 000 000 EUR.

176. **Gelet op deze elementen besluit de Geschillenkamer een uitgangsbedrag vast te stellen van 15 % van het wettelijke maximumbedrag, namelijk 3 000 000 EUR.**

[49] EDPB – Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG, vastgesteld op 24 mei 2023 (v2.1), beschikbaar op: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_nl, zie punt 60.

iii. Omzet van de verwerkingsverantwoordelijke en aanvullende overwegingen waarmee de Geschillenkamer rekening heeft gehouden bij het vaststellen van het bedrag van de geldboete[50]

177. De AVG verplicht elke toezichthoudende autoriteit ervoor te zorgen dat de opgelegde administratieve geldboeten in elke zaak doeltreffend, evenredig en afschrikkend zijn (artikel 83.1 van de AVG).

178. Om dit te bereiken, moeten toezichthoudende autoriteiten de definitie van het begrip "onderneming" toepassen zoals vastgesteld door het Hof van Justitie van de Europese Unie (hierna "HvJ-EU") in het kader van de artikelen 101 en 102 van het VWEU. Volgens deze definitie wordt onder "onderneming" een economische eenheid verstaan, die kan bestaan uit een moedermaatschappij en alle betrokken dochterondernemingen. Overeenkomstig het recht en de rechtspraak van de EU moet een onderneming dus worden beschouwd als een economische eenheid die commerciële/economische activiteiten uitoefent, ongeacht haar rechtsvorm[51]. Het doel is ervoor te zorgen dat de sancties in verhouding staan tot de omvang en de economische macht van de onderneming.

179. Toezichthoudende autoriteiten dienen administratieve geldboeten aan te passen op basis van de ernst van de inbreuk, en dit binnen het bereik zoals vastgelegd in de richtsnoeren van de EDPB, tot aan het wettelijke maximumbedrag. Dit kan leiden tot aanzienlijke verhogingen of verlagingen van het bedrag van de geldboete, afhankelijk van de omstandigheden van het geval.

180. Bovendien bepalen de artikelen 83.4, 83.5 en 83.6 van de AVG dat de totale wereldwijde jaaromzet van het voorgaande boekjaar moet worden gebruikt voor de berekening van de administratieve geldboete. In dit verband moet het begrip "voorgaande" worden uitgelegd overeenkomstig de rechtspraak van het HvJ-EU op het gebied van het mededingingsrecht, zodat het relevante tijdstip voor de berekening van de geldboete het tijdstip is waarop de toezichthoudende autoriteit haar beslissing inzake de geldboete heeft genomen, en niet het tijdstip waarop de bestrafte inbreuk is begaan.

---

[50] EDPB – Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG, vastgesteld op 24 mei 2023 (v2.1), beschikbaar op: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_nl, zie punten 63 tot en met 69; 112 tot en met 131.

[51] De rechtspraak van het Hof van Justitie van de Europese Gemeenschappen geeft de volgende definitie: "*het begrip onderneming* [*omvat*] *elke eenheid* […] *die een economische activiteit uitoefent, ongeacht haar rechtsvorm en de wijze waarop zij wordt gefinancierd*" (zaak C-41/90, *Höfner en Elser/Macrotron,* ECLI:EU:C:1991:161, punt 21). Onder het begrip "onderneming" moet het volgende worden verstaan: "*een* (…) *economische eenheid, ook al wordt deze economische eenheid uit juridisch oogpunt gevormd door verschillende natuurlijke of rechtspersonen*" (zaak C-217/05, *Confederación Española de Empresarios de Estaciones de Servicio,* ECLI:EU:C:2006:784, punt 40). ; HvJ-EU, 10 september 2009, C-97/08 P, *Akzo Nobel NV e.a. t. Commissie*, ECLI:EU:C:2009:536), punten 60-61.

181. Zoals vermeld in punt 160, bedraagt de omzet van de verweerder (.. EUR) voor het jaar 2023. Dit cijfer blijkt uit de jaarrekening van de vzw Y (ondernemingsnummer: [...]) zoals neergelegd bij de Nationale Bank van België (NBB) op [datum] 2024.

182. De Geschillenkamer kan overwegen het uitgangsbedrag aan te passen op basis van de jaaromzet van de onderneming[52]. Voor ondernemingen met een jaaromzet tussen 50 en 100 miljoen EUR laten de richtsnoeren voor de berekening van geldboeten toe dat een aanpassing van de berekening plaatsvindt op basis van een bedrag tussen 8 % en 20 % van het vastgestelde uitgangsbedrag.

183. In het onderhavige geval beslist de Geschillenkamer om het bedrag van 3 000 000 EUR aan te passen tot 13 % van het vastgestelde uitgangsbedrag, wat neerkomt op 390 000 EUR. Deze berekening houdt rekening met de verkorting van de duur van de inbreuk, zoals meegedeeld aan de verweerder in het sanctieformulier. Het uitgangsbedrag bedroeg immers aanvankelijk 400 000 EUR en wordt verlaagd tot 390 000 EUR om rekening te houden met de argumenten die de verweerder in zijn antwoorden op het sanctieformulier heeft aangevoerd.

184. **Gelet op het bovenstaande beslist de Geschillenkamer concreet het uitgangsbedrag voor deze categorie van inbreuken vast te stellen op 390 000 EUR.**

iv. Verzwarende of verzachtende omstandigheden

185. Gelet op artikel 83 van de AVG moet de Geschillenkamer het opleggen van een administratieve geldboete ook concreet motiveren, rekening houdend met andere verzwarende of verzachtende omstandigheden die in artikel 83.2 van de AVG worden opgesomd:

Maatregelen om de schade te beperken (artikel 83.2.c) van de AVG)

186. Zoals vermeld in de richtsnoeren van de EDPB voor de berekening van administratieve geldboeten krachtens de AVG, "zijn verwerkingsverantwoordelijken en verwerkers reeds verplicht “technische en organisatorische maatregelen te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen, effectbeoordelingen inzake gegevensbescherming uit te voeren en de risico’s voor de rechten en vrijheden van personen die voortvloeien uit de verwerking van persoonsgegevens, te beperken”. In het geval van een inbreuk dient de

[52] EDPB – Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG, zie punt 66.

verwerkingsverantwoordelijke of de verwerker echter “al het mogelijke te doen om de gevolgen van de inbreuk voor de betrokkene(n) te beperken”."[53]

187. In dit verband neemt de Geschillenkamer het volgende in aanmerking:

- Wat betreft de verstoring van de spoedeisende hulp: het ziekenhuisnoodplan werd geactiveerd, waardoor patiënten naar andere ziekenhuizen konden worden doorverwezen.
- Wat betreft de onmogelijkheid om toegang te krijgen tot de mailboxen: het ziekenhuis heeft een "patch" geïnstalleerd om het lek in de Exchange-server te verhelpen en om te voorkomen dat een dergelijke inbraak opnieuw kan plaatsvinden.
- Wat betreft de mogelijke diefstal van gevoelige gegevens: het ziekenhuis heeft onmiddellijk de verbindingen van en naar de buitenwereld uitgeschakeld om de omvang van de aanval te beperken.
- Wat betreft de onbeschikbaarheid van de software met de medische dossiers: de verweerder heeft hersteltools geïnstalleerd om de systemen van het ziekenhuis geleidelijk te herstellen. Drie dagen na de aanval was de software voor het beheer van de medische dossiers voor 95 % operationeel.

188. De Geschillenkamer stelt vast dat er maatregelen zijn getroffen om de schade te beperken. Dit criterium vormt een verzachtende omstandigheid.

Gezondheidscontext ten tijde van de inbreuk (artikel 83.2.k) van de AVG)

189. Bij de vaststelling van het bedrag van de geldboete wordt rekening gehouden met de gezondheidscontext ten tijde van de inbreuk, op [datum] 2021. Midden in de COVID-19-crisis werd het ziekenhuis geconfronteerd met een uitzonderlijke situatie, waardoor het zich nog meer moest concentreren op de zorg voor patiënten. Deze ernstige crisis heeft mogelijk de middelen en aandacht beperkt die beschikbaar waren om volledig aan de vereisten van de AVG te voldoen. Dit criterium vormt een verzachtende omstandigheid.

Energiecrisis en inflatie (artikel 83.2.k) van de AVG)

190. Er moet rekening worden gehouden met de uitzonderlijke economische omstandigheden waarmee ziekenhuizen worden geconfronteerd. De energiecrisis en de snel stijgende inflatie hebben namelijk geleid tot een aanzienlijke stijging van de exploitatiekosten, waardoor de financiële druk op de middelen van het ziekenhuis is toegenomen. Deze factoren hebben een rechtstreekse invloed op het vermogen van

[53] EDPB – Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG, zie punt 74.

het ziekenhuis om te investeren in versterkte beveiligingsmaatregelen ter bescherming van persoonsgegevens. Overeenkomstig artikel 83.2.k) van de AVG is het derhalve gerechtvaardigd om deze ongunstige conjunctuur als een verzachtende omstandigheid te beschouwen, wat een aanpassing van de geldboete rechtvaardigt, zodat het financiële evenwicht van het ziekenhuis niet verder in het gedrang komt en het zijn opdrachten onder moeilijke omstandigheden kan blijven vervullen.

191. Ondanks de andere door de verweerder geformuleerde voorstellen waarin de Geschillenkamer werd uitgenodigd om de ernst van de inbreuk anders te beoordelen, evenals een andere interpretatie van de toepasselijke verzwarende en verzachtende omstandigheden, besluit de Geschillenkamer haar analyse van de verzwarende en verzachtende omstandigheden zoals aanvankelijk vastgelegd in het sanctieformulier te handhaven, met één uitzondering[54]. De Geschillenkamer heeft namelijk besloten rekening te houden met de energiecrisis en de inflatie als nieuwe verzachtende omstandigheden. Deze wijziging is meegenomen bij de aanpassing van het uiteindelijke bedrag van de geldboete.

v. Doeltreffend, evenredig en afschrikkend karakter

192. De richtsnoeren van de EDPB herinneren eraan dat de administratieve geldboete die wordt opgelegd voor inbreuken op de AVG zoals bedoeld in artikel 83.4 tot en met artikel 83.6 in elke zaak doeltreffend, evenredig en afschrikkend moet zijn. Toezichthoudende autoriteiten moeten nagaan of het bedrag aan deze criteria voldoet en het indien nodig aanpassen.

▪ Doeltreffendheid

193. Een geldboete wordt als doeltreffend beschouwd als zij de doelstellingen bereikt waarvoor zij is opgelegd, zoals het herstellen van de naleving van de regels, het bestraffen van onrechtmatig gedrag, of beide.

194. In het onderhavige geval is de geldboete bedoeld om het nalatige en ernstige gedrag van de verweerder te bestraffen. Bovendien is zij bedoeld om soortgelijke inbreuken in de toekomst te ontmoedigen. De langdurige aard van de inbreuk, ondanks een eerste gegevensinbreuk in 2019, toont aan dat een krachtige reactie van de Geschillenkamer noodzakelijk is. Het opleggen van een administratieve geldboete

[54] EDPB – Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG, vastgesteld op 24 mei 2023 (v2.1), beschikbaar op: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_nl, zie punt 6.

met een uitgangsbedrag van 390 000 EUR is dan ook een doeltreffende maatregel om deze doelstellingen te verwezenlijken.

▪ **Evenredigheid**

195. Het evenredigheidsbeginsel, zoals gedefinieerd in de AVG, houdt in dat de genomen maatregelen niet verder mogen gaan dan wat passend en noodzakelijk is om de legitieme doelstellingen van de betreffende regelgeving te bereiken. In het geval van geldboeten betekent dit dat het bedrag ervan niet onevenredig mag zijn in verhouding tot de beoogde doelstellingen, de ernst van de inbreuk en de omvang en financiële draagkracht van de betrokken onderneming. Toezichthoudende autoriteiten moeten er dus voor zorgen dat het bedrag van de geldboete in verhouding staat tot de in haar geheel beoordeelde inbreuk, rekening houdend met verschillende factoren, zoals de financiële draagkracht van de onderneming.

196. In bepaalde uitzonderlijke omstandigheden kan een verlaging van de geldboete worden beoogd indien de oplegging ervan de economische levensvatbaarheid van de betrokken onderneming onherstelbaar in gevaar zou brengen. Deze mogelijkheid kan worden beoogd wanneer objectief bewijs aantoont dat de onderneming niet in staat is om te betalen. Bovendien is het van essentieel belang om de risico's te analyseren, rekening houdend met de specifieke sociale en economische context.

197. In het onderhavige geval wijzen verschillende criteria erop dat de voorgestelde geldboete evenredig is:

- ***Economische levensvatbaarheid en financiële draagkracht van de onderneming***: met een geconsolideerde jaaromzet van meer dan 72 miljoen euro voor het boekjaar 2023 beschikt de verweerder over voldoende financiële draagkracht om een geldboete te dragen. Om ervoor te zorgen dat de voorgestelde geldboete de economische levensvatbaarheid van het ziekenhuis niet in gevaar brengt, gelet op de financiële moeilijkheden die door de verweerder met bewijsstukken in het sanctieformulier zijn aangetoond, stemt de Geschillenkamer in met een verlaging van de oorspronkelijk voorgenomen geldboete. Hoewel het uitgangsbedrag van de geldboete van 390 000 EUR slechts ongeveer 0,54 % van een (afgeronde) omzet van 72 000 000 EUR vertegenwoordigt, moet dit bedrag in dit geval met ongeveer een derde worden verminderd, hoofdzakelijk omwille van: (i) de financiële moeilijkheden van het ziekenhuis, in het bijzonder de erkenning als "onderneming in moeilijkheden" en de aanstelling van een crisismanager, en (ii) een bijkomende verzachtende omstandigheid die door de Geschillenkamer in aanmerking is genomen, namelijk de energiecrisis en de inflatie, die eveneens een impact hebben op de financiële draagkracht van de onderneming.
- ***Bewijs van waardeverlies***: er zijn geen aanwijzingen dat het opleggen van de herziene geldboete de levensvatbaarheid van de onderneming in gevaar zou brengen en zou leiden

tot een aanzienlijk verlies van de waarde van haar activa, of haar vermogen om haar activiteiten voort te zetten, in gevaar zou brengen. Er moet een rechtstreeks verband bestaan tussen de geldboete en dat waardeverlies, en het wordt niet automatisch aangenomen dat faillissement of insolventie tot een dergelijk verlies leidt, gelet op het herziene bedrag van de geldboete. Bij gebrek aan dergelijk tastbaar bewijs dat deze correlatie aantoont, lijkt een verdere vermindering van de geldboete niet gerechtvaardigd.

- ***Bijzondere sociale context***: de sociale context van dat moment, gekenmerkt door de COVID-19-gezondheidscrisis in 2021, is een factor waarmee de Geschillenkamer rekening houdt bij het vaststellen van het bedrag van de op te leggen geldboete.

▪ **Afschrikking**

198. Het afschrikkende karakter van de geldboete moet twee dimensies hebben. Zij moet de persoon aan wie de geldboete wordt opgelegd ervan weerhouden om de vastgestelde inbreuken in de toekomst te herhalen, maar ook elke andere persoon ervan weerhouden om het strafbare gedrag van de eerste persoon te herhalen.

199. Verschillende factoren bepalen het afschrikkende karakter van een geldboete: de aard, het bedrag van de geldboete en de waarschijnlijkheid dat deze wordt opgelegd, zijn in dit verband doorslaggevende elementen. Een geldboete moet hoog genoeg zijn om een aanzienlijke financiële impact te hebben op de in overtreding zijnde onderneming, maar moet in verhouding staan tot de ernst van de inbreuk. Met andere woorden, het criterium van afschrikking overlapt met dat van doeltreffendheid.

200. Als een toezichthoudende autoriteit van oordeel is dat een geldboete niet voldoende afschrikkend is, kan zij overwegen deze te verhogen. In sommige gevallen kan zij zelfs een afschrikkingsmultiplicator toepassen om het afschrikkende effect te versterken. Deze multiplicator kan naar goeddunken van de toezichthoudende autoriteit worden aangepast om ervoor te zorgen dat de doelstellingen van afschrikking volledig worden bereikt.

201. **In het onderhavige geval zal, rekening houdend met de herbeoordeling van de duur van de inbreuk, de nieuwe verzachtende omstandigheid die in aanmerking is genomen, evenals de financiële draagkracht van het ziekenhuis, het definitieve bedrag van de geldboete definitief worden herzien tot 200.000 EUR.**

202. Dit bedrag blijft voldoende afschrikkend om te voorkomen dat de verweerder opnieuw de regels van de AVG overtreedt. Bovendien beoogt het ook andere ondernemingen te ontmoedigen om soortgelijke inbreuken te plegen. Deze geldboete, die in verhouding staat tot de ernst van de inbreuk en rekening houdt met de omzet van de verweerder, is bedoeld om zowel een specifiek als een algemeen afschrikkend effect te hebben.

III.3. Over de bevelen tot naleving

203. **Over het opleggen van een maatregel tot naleving**: op grond van artikel 58.2.d) van de AVG en artikel 100, § 9, van de WOG kan de Geschillenkamer de verwerkingsverantwoordelijke bevelen om de verwerkingsactiviteiten in overeenstemming te brengen met de bepalingen van de AVG, in voorkomend geval, op specifieke wijze en binnen een bepaalde termijn.

204. In het onderhavige geval is de Geschillenkamer van oordeel dat bepaalde technische en organisatorische maatregelen, evenals een GEB, op de datum van de beslissing nog steeds niet zijn getroffen. De Geschillenkamer zal de verweerder dan ook bevelen om de in het volgende punt opgesomde bevelen tot naleving uit te voeren.

205. **Bevelen tot naleving**: de Geschillenkamer beveelt de verweerder om binnen een termijn van 90 dagen na de kennisgeving van de beslissing uitvoering te geven aan de volgende punten:

a. een gegevensbeschermingseffectbeoordeling uitvoeren op basis van artikel 35.3 van de AVG. De Geschillenkamer herinnert eraan dat de inhoud van deze GEB ten minste de voorwaarden van artikel 35.7 van de AVG moet bevatten, waaronder een systematische beschrijving van de beoogde verwerkingen en de beoogde maatregelen om de risico's aan te pakken;

b. een "duidelijk en helder beleid voor informatieveiligheid en privacy" invoeren (punt 81 van de beslissing), in overeenstemming met het beleid voor informatieveiligheid van 3 maart 2022, om de beveiliging van de door de verweerder uitgevoerde verwerkingen te waarborgen, overeenkomstig de artikelen 5.1.f) en 32 van de AVG;

c. een regelmatig opleidings-/bewustmakingsprogramma voor werknemers over de AVG opzetten, zodat het ziekenhuis er op zijn minst voor kan zorgen dat al zijn personeel op de hoogte is van de basisbeginselen van de verwerking van persoonsgegevens, waaronder het beginsel van integriteit en vertrouwelijkheid. Deze verplichting vloeit voort uit de toepassing van de artikelen 32, 5.1.f) en 24 van de AVG;

d. de lengte van het wachtwoord voor toegang tot het elektronische patiëntendossier verhogen, teneinde te voldoen aan de artikelen 32, 5.1.f) en 24 van de AVG.

IV. Publicatie van de beslissing

206. Gelet op het belang van transparantie met betrekking tot de besluitvorming van de Geschillenkamer, wordt deze beslissing gepubliceerd op de website van de Gegevensbeschermingsautoriteit. Het is evenwel niet nodig dat daartoe de identificatiegegevens van de verweerder rechtstreeks worden bekendgemaakt.

OM DEZE REDENEN,

beslist de Geschillenkamer van de Gegevensbeschermingsautoriteit, na beraadslaging, om:

- **op grond van artikel 58.2.d) van de AVG en artikel 100, § 1, 9°, van de WOG** de verweerder te bevelen de verwerkingsactiviteiten, wegens schending van de artikelen 35.3, 32, 5.1.f) en 24 van de AVG, in overeenstemming te brengen met de bepalingen van de AVG.
- **op grond van artikel 58.2.i) van de AVG en artikel 100, § 1, 13°, van de WOG**, gelezen in samenhang met artikel 101 van de WOG, de verweerder een administratieve geldboete op te leggen van **200 000 EUR** wegens schending van de artikelen 35.3, 32, 5.1.f) en 24 van de AVG.
- de verweerder te bevelen de Geschillenkamer uiterlijk binnen 30 dagen na de kennisgeving van deze beslissing in kennis te stellen van het gevolg dat aan deze bevelen is gegeven.

207. Tegen deze beslissing kan op grond van artikel 108, § 1, van de WOG, beroep worden aangetekend bij het Marktenhof (hof van beroep van Brussel), binnen een termijn van dertig dagen vanaf de kennisgeving ervan, met de Gegevensbeschermingsautoriteit als verweerder.

208. Een dergelijk beroep kan worden ingesteld door middel van een verzoekschrift op tegenspraak dat de in artikel 1034*ter* van het Gerechtelijk Wetboek (Ger.W.) opgesomde elementen dient te bevatten[55]. Dit verzoek op tegenspraak moet worden ingediend bij de griffie van het Marktenhof overeenkomstig artikel 1034*quinquies* van

[55] Het verzoekschrift vermeldt op straffe van nietigheid:
1° de dag, de maand en het jaar;
2° de naam, de voornaam, de woonplaats van de verzoeker en, in voorkomend geval, zijn hoedanigheid en zijn rijksregisternummer of ondernemingsnummer;
3° de naam, de voornaam, de woonplaats en, in voorkomend geval, de hoedanigheid van de persoon die moet worden opgeroepen;
4° het voorwerp en de korte samenvatting van de middelen van de vordering;
5° de rechter voor wie de vordering aanhangig wordt gemaakt;
6° de handtekening van de verzoeker of van zijn advocaat.

het Ger.W.[56], of via het e-Deposit informaticasysteem van Justitie (artikel 32*ter* van het Ger.W.).

(get.) Hielke HIJMANS

Voorzitter van de Geschillenkamer

[56] Het verzoekschrift met zijn bijlage wordt, in zoveel exemplaren als er betrokken partijen zijn, bij aangetekende brief gezonden aan de griffier van het gerecht of ter griffie neergelegd.