Geschillenkamer

Beslissing ten gronde 101/2022 van 3 juni 2022

Dossiernummer : DOS-2019-04867

Betreft : klacht wegens toekennen telefoonnummer klager aan een derde

De Geschillenkamer van de Gegevensbeschermingsautoriteit, samengesteld uit de heer Hielke Hijmans, voorzitter en de heren Dirk Van Der Kelen en Yves Poullet.

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,* hierna WOG;

Gelet op het reglement van interne orde, 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 klager: De heer X, hierna “de klager”

De verweerder: Y, vertegenwoordigd door Mr. B. Bruyndonckx en Mr. L. Kuyken, beiden kantoorhoudende aan de Havenlaan 86c b113, 1000 Brussel. hierna “de verweerder”

I. Feiten en procedure

Procesverloop

1. Op 22 januari 2021 heeft de Geschillenkamer beslissing 05/2021 genomen jegens verweerder, waarbij aan verweerder een boete van 25.000 EUR is opgelegd wegens inbreuken op de artikelen 5.1.f, 5.2, 24, 32, 33.1 en 5, 34.1 AVG.

- Op 19 februari 2021 heeft verweerder beroep ingesteld tegen beslissing 05/2021 van de Geschillenkamer.

- Op 20 mei 2021 heeft de Geschillenkamer haar beslissing van 22 januari ingetrokken door middel van intrekkingsbeslissing 61/2021 en daarbij beslist om de zaak in heroverweging te zullen nemen middels een nieuwe procedure ten gronde.

- Op 30 juni 2021 sprak het Marktenhof arrest uit in het door Y ingestelde beroep.

- Op 23 september 2021 verstuurde de Geschillenkamer de nieuwe conclusiekalender aan partijen teneinde een nieuwe procedure ten gronde te doen aanvangen.

- Op 2 november 2021 ontving de Geschillenkamer de conclusie van antwoord vanwege de verweerder.

- Op 25 april 2022 wordt de verweerder overeenkomstig artikel 53 van het Reglement van interne orde van de Gegevensbeschermingsautoriteit gehoord door de Geschillenkamer.

2. Deze beslissing komt tot stand op basis van een nieuwe procedure ten gronde. De Geschillenkamer heeft haar primaire beslissing 05/2021 naar aanleiding van de klacht in onderhavig dossier immers ingetrokken en heeft beslist over te gaan tot een nieuwe procedure ten gronde. Onderhavige beslissing wordt derhalve genomen op basis van de klacht, de ingediende verweermiddelen en de overige relevante stukken van het geding.

De klacht en de primaire beslissing op de klacht door de Geschillenkamer

3. Klager diende op 20 september 2019 een klacht tegen Y in bij de Gegevensbeschermingsautoriteit. De klacht is op 30 september 2019 ontvankelijk verklaard door de Eerstelijnsdienst. De klacht hield in dat het mobiele telefoonnummer van klager door zijn provider Y zou zijn toegekend aan een derde waardoor klager niet meer over zijn nummer kon beschikken. De simkaart van klager werd gedeactiveerd en de derde zou dus kennis hebben kunnen nemen van het persoonlijk GSM-verkeer en oproepen van de klager, alsmede gekoppelde accounts (zoals Paypal, WhatsApp en Facebook) van 16 tot en met 19 september 2019.

4. Op 15 april 2020 heeft de Geschillenkamer beslist dat de klacht gereed was voor behandeling ten gronde en zowel de klager als de verweerder per aangetekende zending in kennis gesteld van deze beslissing. Tevens werden de partijen in kennis gesteld van de bepalingen zoals vermeld in artikel 98 van de WOG en de termijnen om hun verweermiddelen in te dienen. De uiterste datum voor ontvangst van de conclusie van antwoord van verweerder werd bepaald op 27 mei 2020; de uiterste datum voor ontvangst van de conclusie van repliek van de klager op 17 juni 2020 en de uiterste datum voor ontvangst van de conclusie van repliek van verweerder op 8 juli 2020. Op 27 mei 2020 heeft verweerder een conclusie van antwoord neergelegd. Op 9 november 2020 wordt de verweerder overeenkomstig artikel 53 van het Reglement van interne orde gehoord door de Geschillenkamer. Op 19 november 2020 wordt het proces-verbaal van de hoorzitting aan partijen voorgelegd. Op 7 december 2020 is het voornemen tot het opleggen van een geldboete overgemaakt aan de verweerder. Op dit voornemen heeft verweerder op 22 december 2020 uitgebreid gereageerd.

5. Vervolgens heeft de Geschillenkamer op 22 januari 2021 beslissing 05/2021 genomen en de verweerder een geldboete opgelegd van 25.000 EUR wegens schending van de artikelen 5.1.f, 5.2, 24, 32, 33.1 en 5, 34.1 AVG.

6. Op 19 februari 2021 stelde Y beroep in bij het Marktenhof tegen de beslissing van de Geschillenkamer van 22 januari 2021. Y stelde in het beroep dat de Geschillenkamer bij het nemen van de beslissing de rechten van verdediging had miskend en de beginselen van behoorlijk bestuur had geschonden. Verweerder stelde onder meer dat het evenredigheidsbeginsel was geschonden omdat de Geschillenkamer geen onderzoek had gevraagd aan de Inspectiedienst. De Geschillenkamer schond volgens verweerder eveneens het motiveringsbeginsel en het beginsel van redelijkheid, door een volgens verweerder disproportionele beslissing met een hoge geldboete te nemen. De verweerder was van mening dat de rechten van verdediging werden geschonden door verweerder geen kans te geven om zijn standpunten kenbaar te maken op basis van een concrete tenlastelegging. De Geschillenkamer was volgens verweerder ten onrechte tot de conclusie gekomen dat er sprake was van inbreuken op de artikelen 5.1.f, 5.2, 24, 32, 33.1 en 5, als ook 34.1 AVG.

7. Hangende het beroep werd bovengenoemde beslissing door de Geschillenkamer ingetrokken door de intrekkingsbeslissing 61/2021. In die beslissing overwoog de Geschillenkamer als volgt :

"Overwegende dat het Marktenhof in zijn uitspraken 2020/AR/813 van 18 november 2020 en 2021/AR/1159 van 24 februari 2021 gewezen heeft op het belang om betrokkenen voorafgaand aan de behandeling van het dossier in te lichten over de exacte aantijgingen en/of inbreuken waaraan hij zich schuldig zou kunnen maken; Overwegende dat Y NV tijdens het beroep bij het Marktenhof tegen de beslissing ten gronde 5/2021 van 22 januari 2021 heeft gesteld dat zij in de aan deze beslissing voorafgaande procedure onvoldoende is ingelicht omtrent de exacte aantijgingen en/of inbreuken.

Heeft beslist om:
. de beslissing ten gronde 5/2021 van 22 januari 2021 gericht tegen Y NV middels onderhavige beslissing in te trekken.
. de procedure voor de Geschillenkamer te heropenen en de partijen met inachtneming van het bepaalde in artikel 98 van de GBA-Wet te verzoeken nieuwe verweermiddelen in te dienen."

8. Tegen de intrekkingsbeslissing van de Geschillenkamer werd door verweerder geen beroep ingesteld. Verweerder vorderde tijdens de behandeling van het beroep tegen de primaire beslissing van de Geschillenkamer echter dat het Marktenhof "*Opnieuw rechtdoende en met gebruikmaking van haar volheid van rechtsmacht, de grond van de zaak zou moeten beoordelen en haar eigen beslissing in de plaats diende te stellen van de Geschillenkamer."*

9. Op 30 juni 2021 velde het Marktenhof arrest. Daarin overwoog het hof echter als volgt omtrent het bovengenoemd verzoek van verweerder *:*

" Nu de beslissing van 19 mei 2021 stelt dat er is beslist "om de procedure voor de Geschillenkamer te heropenen en de partijen met inachtneming van het bepaalde in artikel 98 van de GBA-Wet te verzoeken nieuwe verweermiddelen in te dienen" en hiertegen geen verhaal is ingesteld, heeft Y ermede ingestemd dat het Marktenhof te dezen hic et nunc geen eigen beslissing kan nemen en dat vooreerst de Geschillenkamer de gelegenheid moet krijgen om de procedure te hervatten."[1]

10. Met het bovenstaande heeft het Marktenhof derhalve bevestigd dat de beslissing van de Geschillenkamer waartegen beroep werd ingesteld door verweerder niet meer bestaat in het rechtsverkeer en deze door de intrekkingsbeslissing geacht wordt nooit te hebben bestaan. De vordering van verweerder dat het Marktenhof uit hoofde van zijn volle rechtsmacht een eigen beslissing zou moeten nemen door zich in de plaats van de Geschillenkamer te stellen werd door het Marktenhof derhalve ongegrond verklaard. Het beroep is zonder voorwerp.

[1] Overweging 7.5 arrest Marktenthof

11. Het Marktenhof heeft daarnaast opgemerkt dat de intrekking van de beslissing op zich niet kan worden aanzien als een bewijs dat de Geschillenkamer een *verkeerde* of *onwettige* beslissing heeft genomen. Volgens het Marktenhof is er evenmin sprake van enig foutief gedrag in hoofde van de Geschillenkamer. Integendeel, de intrekking getuigt volgens het Marktenhof van eerbiediging van de principes van de rechtstaat door de Geschillenkamer.

Nieuwe procedure ten gronde

12. Op 23 september 2021 heeft de Geschillenkamer een nieuwe conclusiekalender verzonden aan partijen. In dit schrijven werd door de Geschillenkamer eveneens een opsomming gegeven van de aan verweerder ten laste gelegde feiten welke als volgt luidden: "Verweerder wordt ten laste gelegd dat:

1. hij geen, dan wel een onvolledige of onjuiste verificatie heeft uitgevoerd bij het nagaan of de derde persoon die in de winkel van verweerder verzocht om een migratie van zijn simkaart van prepaid naar postpaid en aangaf de houder van het telefoonnummer te zijn ook daadwerkelijk die persoon was. Ten gevolge van het voorgaande werd zijn[2] nummer toegekend aan de derde en kon de derde beschikken over het telefoonnummer en kennis nemen van het telefoonverkeer van klager waardoor er sprake was van een gegevenslek. Derhalve wordt aan verweerder ten laste gelegd dat hij niet de nodige technische en organisatorische maatregelen zou hebben getroffen teneinde een schending van de privacy van klager te voorkomen (artikelen 5.1.f, 5.2, 24 en 32 AVG)

2. hij het gegevenslek welke is ontstaan ten gevolge van de onder 1 omschreven handelswijze niet heeft gemeld aan de Gegevensbeschermingsautoriteit noch aan de betrokkene, in casu klager (artikelen 33.1, 33.5 en 34.1 AVG)"

13. De Geschillenkamer formuleerde daarnaast de navolgende vragen teneinde meer duidelijkheid te verkrijgen:

"1. Heeft de verweerder alle nodige technische en organisatorische maatregelen conform de artikelen 5.1.f, 24 en 32 AVG getroffen en een passend niveau van beveiliging geboden teneinde te voorkomen dat het -beweerdelijk- toekennen van het telefoonnummer van klager aan een derde kon gebeuren en zo ja, kan zij dit aantonen ?

2. Kan verweerder aantonen proactieve maatregelen te hebben genomen conform artikel 5.2 AVG teneinde de naleving van de voorschriften van de AVG -waaronder de hierboven onder 1 vermelde maatregelen- te waarborgen ?

[2] Bedoeld wordt het telefoonnummer van de klager

3. Was er volgens verweerder sprake van een gegevenslek, en heeft verweerder in dat geval voldaan aan de plicht om melding te maken van dat gegevenslek aan de Gegevensbeschermingsautoriteit conform artikel 33.1 AVG en heeft zij deze inbreuken gedocumenteerd conform artikel 33.5 AVG als ook melding daarvan gedaan aan de betrokkene conform artikel 34.1 AVG ?

14. De termijnen om verweermiddelen in te dienen werden bepaald op :

- 2 november 2021 als uiterste datum voor ontvangst van de conclusie van antwoord van verweerder;
- 23 november 2021 als uiterste datum voor ontvangst van de conclusie van repliek klager;
- 14 december 2021 als uiterste datum voor ontvangst van de conclusie van repliek van verweerder.

15. De Geschillenkamer ontving op 2 november 2021 de conclusie van antwoord van verweerder waarin de volgende middelen naar voren worden gebracht:

- Verweerder nam alle nodige technische en organisatorische maatregelen conform de artikelen 5 (1) (f), 24 en 32 van de AVG en bood een passend niveau van beveiliging;
- Verweerder nam proactieve maatregelen conform artikel 5 (2) van de AVG teneinde de naleving van de voorschriften van de AVG, waaronder de technische en organisatorische maatregelen te waarborgen;
- Verweerder handelde conform de artikelen 33 en 34 van de AVG;
- De Geschillenkamer zal volgens verweerder moeten zetelen in een geheel andere samenstelling gezien het arrest van het Marktenhof waarin dat werd bepaald. Indien de samenstelling van de Geschillenkamer in deze procedure niet volledig zou verschillen van de samenstelling van de Geschillenkamer die uitspraak deed op 22 januari 2021, is de samenstelling volgens verweerder onregelmatig en de procedure al evenzeer.

16. Op 25 april 2022 worden partijen door de Geschillenkamer gehoord.

17. Op 9 mei 2022 wordt het proces-verbaal van de zitting overgemaakt aan de partijen.

18. Op 17 mei 2022 ontvangt de Geschillenkamer de opmerkingen vanwege de verweerder op het proces-verbaal. Allereerst stelt verweerder dat de voorzitter Hielke Hijmans tijdens de hoorzitting zou hebben “toegegeven” dat de beslissing van het Marktenhof waarin werd bepaald dat de Geschillenkamer dient te zetelen in een geheel andere samenstelling indien een zaak een tweede keer door de Geschillenkamer wordt behandeld, zoals *in casu* het geval is, niet door de Geschillenkamer zou zijn gerespecteerd. Tevens is verweerder van mening dat het proces-verbaal onvoldoende weergeeft wat de leden tijdens de zitting naar voren gebracht zouden hebben. Hierbij wordt niet gepreciseerd wat zou ontbreken.

19. Op 16 mei 2022 is het sanctieformulier aan verweerder verzonden.

20. Op 31 mei ontvangt de Geschillenkamer de reactie van verweerder op het sanctieformulier.

De inhoud van de zaak

21. Klager is sinds 11 juni 2015 klant bij verweerder en neemt (prepaid) mobiele telefoondiensten af. Het telefoonnummer van klager is voor de duur van vier dagen, te weten van 15 tot en met 19 september 2019, toegekend aan een derde waarbij de simkaart van klager is gedeactiveerd.

22. De Geschillenkamer heeft tijdens deze procedure getracht zicht te verkrijgen op het verloop van de gebeurtenissen die hebben geleid tot het toekennen van het telefoonnummer van klager aan een derde. Uit deze beslissing wordt duidelijk dat het één en ander omtrent het feitelijk verloop niet geheel kan worden uitgeklaard. Volgens verweerder is de derde op 11 september 2019 in één van de winkels van verweerder geweest teneinde het prepaid-abonnement van klager om te laten zetten in een postpaid-abonnement met bijhorend smartphonetoestel dat na 24 maanden abonnement is afbetaald. Daarbij werd volgens verweerder zowel het telefoonnummer als het simkaartnummer van de klager opgegeven door de derde. Vanaf 11 september 2019 veranderde het abonnement van klager derhalve van prepaid naar postpaid. De derde heeft wel zijn eigen identiteitsgegevens opgegeven waardoor deze werden gekoppeld aan het postpaid-abonnement zodat alle kosten vanaf dat moment op de naam van de derde werden gefactureerd. De derde beschikte op 11 september 2019 echter nog niet over een simkaart verbonden aan het gsm-nummer van de klager waardoor klager nog zelf kon blijven gebruik maken van de diensten van het abonnement. Vier dagen later, op 15 september 2019, is de derde volgens verweerder opnieuw naar een Y-shop geweest en heeft gevraagd om een nieuwe simkaart verbonden aan hetzelfde gsm-nummer. Op dat ogenblik kreeg hij dus toegang tot het gsm-nummer van de klager en werd de simkaart van klager afgesloten. De klager had geen contact meer met het netwerk vanaf dat moment.

23. Klager omschrijft in zijn klacht meerdere keren telefonisch contact met verweerder te hebben gehad en in de winkels van verweerder te zijn geweest teneinde opnieuw te kunnen beschikken over zijn telefoonnummer. Het was pas op 19 september 2019 dat klager opnieuw kon beschikken over zijn telefoonnummer.

II. Motivering

2.1 Over de samenstelling van de Geschillenkamer

24. Verweerder heeft zowel bij conclusie als tijdens de hoorzitting uitdrukkelijk voorbehoud gemaakt wat betreft de samenstelling van de Geschillenkamer. Verweerder wees er tijdens de hoorzitting op dat de samenstelling van de Geschillenkamer niet in zijn totaliteit uit andere fysieke personen

bestond en merkte op dat de twee leden waren vervangen terwijl de voorzitter in deze procedure bleef zetelen. Verweerder heeft bovendien in zijn reactie op het proces- verbaal te kennen gegeven dat de voorzitter zou hebben toegegeven zich niet aan de uitspraak van het Marktenhof te houden. Voorgaande bewering is onjuist. De Geschillenkamer zal hieronder met redenen omkleed uiteen zetten waarom is gekozen voor deze samenstelling van de Geschillenkamer bij de behandeling van dit dossier.

25. Het Marktenhof besliste in zijn arrest van 30 juni 2021 immers dat de Geschillenkamer "*in haar totaliteit zou samengesteld zijn door andere fysieke personen dan deze die deel uitmaakten van de kamer* bij *het nemen van de thans bestreden beslissing."* Verweerder stelt daarom dat de procedure onrechtmatig is indien de Geschillenkamer niet is samengesteld door drie andere personen dan diegenen die deel uitmaakten van de Geschillenkamer bij het nemen van de primaire beslissing.

26. Het hof oordeelde voorts dat : "*Hoewel de leden van de Geschillenkamer geen rechters zijn past het dat dit orgaan de basisregels van behoorlijk bestuur zou naleven met inbegrip van minstens de schijn te* wekken *van onpartijdigheid".*

27. De Geschillenkamer benadrukt dat *in casu* geen sprake is van enige door het Marktenhof vastgestelde onwettigheid van het handelen van de Geschillenkamer. Van een arrest waarin de onpartijdigheid van de Geschillenkamer in vraag wordt gesteld is al helemaal geen sprake. Het tegendeel is waar. De Geschillenkamer heeft ervoor gekozen om zijn eerste beslissing in trekken met de motivering :

> *"Overwegende dat het Marktenhof in zijn uitspraken 2020/AR/813 van 18 november 2020 en 2021/AR/1159 van 24 februari 2021 gewezen heeft op het belang om betrokkenen voorafgaand aan de behandeling van het dossier in te lichten over de exacte aantijgingen en/of inbreuken waaraan hij zich schuldig zou kunnen maken; Overwegende dat Y NV tijdens het beroep bij het Marktenhof tegen de beslissing ten gronde 5/2021 van 22 januari 2021 heeft gesteld dat zij in de aan deze beslissing voorafgaande procedure onvoldoende is ingelicht omtrent de exacte aantijgingen en/of inbreuken."*

28. Er is geen enkele aanwijzing dat de Geschillenkamer - zoals zij eerst samengesteld was - partijdig zou zijn en niet (in gedeeltelijk of zelfs geheel dezelfde samenstelling) opnieuw zou kunnen oordelen over de zaak.

29. Tegen de intrekkingsbeslissing van de Geschillenkamer werd bovendien geen beroep aangetekend door verweerder. Verweerder verzocht het Marktenhof om zijn eigen beslissing in de plaats te stellen van die van de Geschillenkamer en uitspraak te doen over de grond van het beroep, welke door haar was ingesteld tegen de primaire beslissing en die hangende het beroep door de Geschillenkamer werd ingetrokken. Het Marktenhof wees het verzoek van verweerder

af en overwoog daarbij dat door de intrekkingsbeslissing van de Geschillenkamer de bestreden beslissing werd geacht nooit te hebben bestaan in het rechtsverkeer. Daarmee was het beroep zonder voorwerp geworden. Het Hof merkte daarbij eveneens op dat de intrekking van de beslissing op zich niet kan worden aanzien als een bewijs dat de Geschillenkamer een *verkeerde* of *onwettige* beslissing heeft genomen. De intrekking van de beslissing getuigt volgens het Marktenhof van eerbiediging van de principes van de rechtstaat door de Geschillenkamer.

30. Het Marktenhof sprak zich in een arrest van 7 augustus 2018 principieel uit over de vraag of een zaak, na vernietiging wegens een procedureel gebrek, dient te worden herbeoordeeld door een anders samengesteld orgaan, dan wel of het orgaan in dezelfde samenstelling een nieuwe beslissing mag nemen. Het betrof een beslissing van de Belgische Mededingingsautoriteit (BMA). Het Marktenhof besliste in dit arrest dat een andere samenstelling in dat geval noodzakelijk was, omdat artikel IV.30 Wetboek van Economisch Recht (WER) artikel 828 Gerechtelijk Wetboek (Ger. W.) toepasselijk verklaart op de BMA. In artikel 828 Ger. W. zijn de wrakingsgronden voor rechters opgenomen. Van cruciaal belang in dat arrest was dat het Marktenhof oordeelde dat artikel 828 Ger. W. *enkel* kan worden toegepast op andere personen dan de rechters behorend tot de rechterlijke macht indien de wet dat uitdrukkelijk zo voorziet. Aangezien de WOG geen bepaling bevat die artikel 828 Ger. W. van toepassing verklaart op de leden van de Geschillenkamer, kunnen leden van de Geschillenkamer niet op grond van deze bepaling worden gewraakt indien zij reeds eerder kennis hebben genomen van hetzelfde geschil.

31. De Geschillenkamer spant zich maximaal in en doet al het mogelijke om het onpartijdigheidsbeginsel als algemeen beginsel van behoorlijk bestuur in acht te nemen, teneinde een eerlijk proces voor de partijen te garanderen. Dit beginsel waarborgt immers zowel de persoonlijke onpartijdigheid van de leden van de Geschillenkamer die een beslissing nemen, als de structurele onpartijdigheid van de Geschillenkamer op het vlak van de organisatie ervan, het verloop van de procedure en het tot stand komen van haar beslissingen.[3]

32. Het onpartijdigheidsbeginsel is volgens vaste rechtspraak van de Raad van State echter slechts van toepassing op de organen van het actief bestuur "*voor zover dit verenigbaar is met de eigen aard, in het bijzonder de structuur van de overheid*".[4] De toepassing van het beginsel mag er meer bepaald niet toe leiden dat het nemen van een regelmatige beslissing onmogelijk wordt, namelijk doordat dit beginsel het optreden van het bevoegde bestuursorgaan onmogelijk zou maken.[5] In de mate dat de toepassing van het beginsel ertoe zou leiden dat bijvoorbeeld een orgaan zijn wettelijke bevoegdheden niet meer zou kunnen uitoefenen, zal de toepassing van dit beginsel opzij worden geschoven.

---

[3] Zie, naar analogie, RvS 26 februari 2015, nr. 230.338, *Deputatie van de provincieraad van Antwerpen*, overw. 10.

[4] Zie bv. RvS 3 oktober 2014, nr. 228.633, *ASBL Unsolicited Artists*; 10 december 2020, nr. 249.191, overw. 25.

33. De Geschillenkamer bestaat uit een voorzitter en zes leden waarvan drie Nederlandstalige en drie Franstalige.[6] Deze leden hebben allen hun eigen expertisegebied. Bij de behandeling van een dossier voor de Geschillenkamer worden de leden derhalve betrokken op basis van de taal die zij spreken en hun deskundigheid waar een beroep op wordt gedaan. Het onpartijdigheidsbeginsel is zoals hierboven aangegeven van toepassing voor zover dit verenigbaar is met de aard en de structuur van de overheid. De twee Nederlandstalige leden Frank De Smet en Jelle Stassijns zetelden tezamen met de voorzitter ten tijde van de primaire behandeling van de klacht tegen verweerder. Dit betekent dat er slechts 1 Nederlandstalig lid overblijft. Het is om die reden alleen al voor de Geschillenkamer niet mogelijk te zetelen in een geheel andere samenstelling aangezien dit simpelweg niet verenigbaar is met de aard en de structuur van de Geschillenkamer en het de continuïteit van de Geschillenkamer ernstig in de weg zou staan. Aangezien kennis van de taal waarin een klacht voor de Geschillenkamer wordt behandeld onontbeerlijk is voor een efficiënte wijze van behandeling worden de leden voor de behandeling van een bepaald dossier in eerste instantie aangewezen door de voorzitter – overeenkomstig artikel 33 WOG en artikel 43 van het Regelement van interne orde - op basis van de gesproken taal en uiteraard expertise op desbetreffend vlak. Wat betreft de taalrol is het uitgangspunt dat - naast de voorzitter die voldoet aan de taalvereisten voor alle landstalen – ten minste één lid behoort tot de taalrol van de taal van de procedure (en het ander lid afdoende feitelijke kennis van de taal heeft).

34. De Geschillenkamer herinnert eraan dat het beginsel van behoorlijk bestuur van onpartijdigheid volgens de rechtsleer minder vergaand en minder streng is dan het beginsel van behoorlijke rechtsbedeling dat geldt voor de rechter. De bestuurde heeft namelijk in ieder geval altijd de mogelijkheid een beroep in te dienen bij een rechter die voldoet aan de eisen van artikel 6.1 EVRM.[7]

35. Het Hof van Justitie oordeelde dat zelfs de samenstelling van een *rechtsprekende* formatie niet volledig dient te worden gewijzigd na terugverwijzing.[8] Volgens het Hof "*kan het feit dat een en dezelfde rechter zitting houdt in twee rechtsprekende formaties [van het Gerecht] die* achtereenvolgens *kennis hebben genomen van dezelfde zaak, op zich, los van elk ander objectief element, geen twijfel over de onpartijdigheid van het Gerecht doen rijzen.*" "*Niets wijst erop dat de verwijzing van de zaak naar een rechtsprekende formatie die op een totaal andere wijze is samengesteld dan die welke als eerste kennis heeft genomen van de zaak, in het kader van het gemeenschapsrecht als een algemene verplichting moet of kan worden beschouwd.*"

36. Ter staving van hun oordeel verwijzen de Unierechters naar de rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM), dat reeds meermaals heeft geoordeeld dat "*uit het*

[6] Artikel 40 § 1 Wet Oprichting Gegevensbeschermingsautoriteit

[7] RvS 23 april 2009, nr. 192.590, *Crauwels*, overw. 3.2.4. Zie ook I. OPDEBEEK en S. DE SOMER, *Algemeen bestuursrecht. Grondslagen en beginselen*, Antwerpen, Intersentia, 2017, 384-385.

[8] H.v.J., C-341/06 P en C-342/06 P, *Chronopost en La Poste/UFEX e.a.*, 1 juli 2008, EU:C:2008:375, §§ 51-60.

onpartijdigheidsvereiste niet het algemene beginsel kan worden afgeleid dat een rechterlijke instantie die een administratieve of rechterlijke beslissing vernietigt, verplicht is de zaak naar een andere instantie of naar een uit andere personen samengesteld orgaan van deze instantie te verwijzen". Zo heeft het EHRM met betrekking tot een tuchtcollege geoordeeld, dat de omstandigheid dat drie van de zeven leden van dat college, nadat een eerdere uitspraak waarbij zij betrokken waren geweest, in cassatie was vernietigd, na verwijzing opnieuw over dezelfde zaak moesten oordelen, geen legitieme vrees voor partijdigheid opleverde.[9]

37. Alhoewel er geen sprake is van een vastgestelde onwettigheid van het handelen van de Geschillenkamer of twijfels over de onpartijdigheid van de Geschillenkamer, heeft de voorzitter van de Geschillenkamer beslist om zoveel mogelijk tegemoet te komen aan het verzoek van verweerder en *in casu* twee andere leden aangewezen - namelijk de heer Dirk Van Der Kelen en de heer Yves Poullet - om te zetelen bij de behandeling van onderhavige procedure ten gronde. De voorzitter zal derhalve zelf blijven zetelen nu het voor de Geschillenkamer praktisch gezien onhaalbaar is om te zetelen in een totaal andere samenstelling, rekening houdend met het aantal leden van beide taalrollen.

2.2 Verweermiddelen en analyse Geschillenkamer

Eerste middel: Verweerder heeft alle nodige technische en organisatorische maatregelen getroffen conform de artikelen 5 (1) (f), 24 en 32 van de AVG en daarmee een passend niveau van beveiliging geboden.

38. Verweerder voert als eerste middel aan alle nodige technische en organisatorische maatregelen te hebben getroffen conform de artikelen 5 (1) (f), 24 en 32 van de AVG en daarmee een passend niveau van beveiliging te hebben geboden. Dat er een passend niveau van beveiliging werd geboden kan volgens verweerder worden aangetoond aan de hand van een aantal aspecten. Allereerst hanteert verweerder interne regels betreffende de technische en organisatorische maatregelen welke nagekomen dienen te worden binnen de organisatie. Verweerder neemt te allen tijde de gepaste technische en organisatorische maatregelen om de persoonsgegevens van haar abonnees te beveiligen. De getroffen maatregelen worden ieder jaar geëvalueerd en indien nodig aangepast. Tevens voert het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT) een jaarlijkse audit uit naar de technische en organisatorische maatregelen binnen de organisatie. Vanwege de vertrouwelijkheid ervan kan het document volgens verweerder niet in deze procedure worden ingebracht. Bovendien heeft verweerder een plicht tot geheimhouding van communicatie welke voortvloeit uit artikel 124 Wet Elektronische Communicatie (WEC).

[9] EHRM, *Diennet t. Frankrijk*, 26 september 1995, § 38.

39. De documenten *YBelgium overzicht van Technische en Organisatorische maatregelen en Group Security Standard*[10] zijn nieuwe documenten waar de Geschillenkamer niet eerder kennis van had kunnen nemen. Het document Group Security Standard bevat de verplicht te nemen veiligheidsmaatregelen van de *Y Group*. Het betreft een gedeeld referentiepunt van *Y Group* en beschrijft de minimale verplicht door elke entiteit te implementeren beveiligingseisen. Het document bevat algemene principes inzake veiligheid, informatieveiligheid en fysieke veiligheid. Ook het document Y *Belgium overzicht van Technische en Organisatorische maatregelen* bevat algemene principes.

Omtrent de verificatie van de identiteit

40. Verweerder heeft bij conclusie en tijdens de hoorzitting te kennen gegeven dat het niet mogelijk was om de identiteit van de derde en die van de houder van het nummer verbonden aan het prepaid-abonnement met elkaar te vergelijken. Verweerder wijst er echter op dat de interne procedure is gewijzigd naar aanleiding van de beslissing van 22 januari 2021 van de Geschillenkamer waarin onder andere werd bevolen om de verwerking in overeenstemming te brengen met de artikelen 24 en 32 AVG. Verweerder hanteert sindsdien derhalve als standaardprocedure dat er wel een verificatie wordt uitgevoerd van de identiteit bij omzetting van prepaid- naar postpaidkaarten. Daarbij is aan medewerkers in de shops toegang gegeven tot het uitvoeren van die controle. De reden dat eerder geen verificatiecontroles werden uitgevoerd heeft volgens verweerder alles te maken met de verboden die zijn opgelegd door artikel 127 van de Wet Elektronische Communicatie en het uitvoerend Koninklijk Besluit[11]. Het uitvoerend besluit bevat nadere regels omtrent de identificatie van de eindgebruikers van voorafbetaalde (prepaid) kaarten.[12] Volgens verweerder schrijven de wet en de besluiten voor dat identificatiegegevens niet mogen gebruikt worden voor commerciële doeleinden. Verweerder stelt namelijk : "*Door de strikte toepassing van bovenstaande wetgeving kunnen medewerkers in de verkooppunten van concluante bij het verzoek van de migratie van een prepaid- naar een postpaid-abonnement enkel het telefoonnummer en het simkaartnummer nagaan*."

41. Het door verweerder geciteerde deel uit de preambule bij het Koninklijk Besluit luidt: "*De operatoren en de aanbieders bedoeld in artikel 126, § 1, eerste lid, mogen bijgevolg de identificatiegegevens die worden verzameld krachtens artikel 127 van de WEC en die worden bewaard krachtens artikel 126 van de WEC niet gebruiken voor commerciële doeleinden .....*".

[10] Deze documenten zijn bij conclusie ingebracht in de procedure.

[11] *Wet betreffende de elektronische communicatie* van 13 juni 2005, in werking getreden op 30 juni 2005 en uitvoerend Koninklijk besluit

[12] Koninklijk Besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart, *BS* 7 december 2016.

De Geschillenkamer wijst erop dat voornoemd artikel echter als volgt wordt vervolgd *: 'maar ze mogen identificatiegegevens van gebruikers van voorafbetaalde kaarten verzamelen en bewaren voor commerciële doeleinden in overeenstemming met artikel 122 (van toepassing wanneer een factuur wordt verstuurd) of de algemene wetgeving rond de bescherming van de persoonlijke levenssfeer.*"

42. Tijdens de hoorzitting heeft verweerder aangaande bovengenoemd artikel 127 WEC, gelezen in samenhang met het uitvoerend Koninklijk Besluit en het Verslag aan de Koning bij dat besluit, aangegeven dat de bepaling bij alle telecomoperatoren aanleiding heeft gegeven tot discussie, namelijk of het artikel strikt moet gelezen worden of niet. Verweerder interpreteert het wetsartikel strikt. Aangezien het *in casu* zou gaan over de verkoop van abonnementen, wordt dit door verweerder als een commerciële doelstelling beschouwd.

43. De stelling van verweerder dat het uitvoeren van een identiteitscontrole (dus *in casu* het vergelijken van de identiteitsgegevens van de klager en de derde) in het kader van een omzetting van prepaid- naar een postpaid-abonnement, niet mocht plaatsvinden vanwege het wettelijk verbod op het gebruik voor commerciële doeleinden, acht de Geschillenkamer onjuist.

44. De Geschillenkamer is, in tegensteling tot verweerder, van oordeel dat hier geen sprake is van een commercieel doeleinde. Allereerst is het doel van het gebruik van de identiteitsgegevens van een prepaid-klant *in casu* enkel het voorkomen van misbruik van het telefoonnummer door eventuele onbevoegden, zoals in onderhavig geval. Het doeleinde is dus het voorkomen van het onterecht overnemen van een telefoonnummer van een prepaid-klant door een derde, waardoor deze ook toegang zou krijgen tot zijn gsm-verkeer en mogelijk ook andere diensten gekoppeld aan het telefoonnummer. Derhalve had verweerder de gegevens van de derde en de bij hem bekende gegevens van klager op een ondubbelzinnige manier moeten vergelijken (en dus niet alleen op basis van een simkaartnummer dat allesbehalve een sterk identificatiemiddel is. Kortom, het gaat hier om een gerechtvaardigd doeleinde, namelijk het detecteren van mogelijke fraude met telefoonnummers welke enorme gevolgen voor betrokkenen kan hebben.

45. Hierbij wijst de Geschillenkamer tevens op het Verslag aan de Koning bij het uitvoerend Koninklijk Besluit.[13] In het verslag is het volgende te lezen: "*Het is de bedoeling van de wetgever hierbij niet geweest om een algeheel verbod op identiteitscontrole op te leggen maar deze aan strikte regelgeving te onderwerpen teneinde een goed beschermingsniveau van persoonsgegevens te kunnen garanderen.*" Door geen controle uit te voeren is verweerder voorbijgegaan aan de wil van de wetgever, namelijk het bieden van een goed beschermingsniveau van persoonsgegevens aan betrokkenen. In een geval als dit strekt de –

[13] Verslag aan de Koning bij Koninklijk Besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart, *BS* 7 december 2016.

beperkte - verwerking van persoonsgegevens ter controle van de identiteit er juist toe om misbruik van persoonsgegevens te voorkomen.

46. De verweerder stelt bij conclusie voorts:

"Indien de Geschillenkamer evenwel meent dat concluante toch verplicht was om de identiteit te vergelijken met de identiteit van de houder van het telefoonnummer, interpreteert zij de regelgeving en de richtlijnen waaraan de verwerkingsverantwoordelijke is onderworpen bijzonder soepel. Op geen enkele manier blijkt dat dit de bedoeling van de wetgever zou zijn, waardoor van concluante niet kon verwacht worden dat zij dergelijke mening was toegedaan."

47. In tegenstelling tot de stelling van verweerder oordeelt de Geschillenkamer dat artikel 18 § 1 van het Koninklijk Besluit dat uitvoering en uitleg geeft aan artikel 127 § 1 van de WEC zeer duidelijk is en geen ruimte overlaat voor twijfel over de interpretatie en toepassing ervan. Het artikel bepaalt namelijk :

"De betrokken onderneming vergewist zich ervan, door technische en operationele maatregelen in te stellen, dat de persoon die de uitbreiding of de migratie van het product vraagt, daadwerkelijk de voor dat product geïdentificeerde persoon is."

48. Vervolgens geeft de artikelsgewijze bespreking van het Koninklijk Besluit de volgende duidelijke uitleg aan dit artikel:

"Art. 18. Productuitbreiding of –migratie. Het is mogelijk dat een persoon al klant is bij een betrokken onderneming voor een ander product (bijvoorbeeld een abonnement op mobiele telefonie) en door de betrokken onderneming geïdentificeerd is voor dat product. Die persoon kan dan beslissen om aanvullend een voorafbetaalde kaart te kopen (productuitbreiding) of om van het eerste product over te stappen naar een voorafbetaalde kaart (productmigratie).De betrokken onderneming kan dan een link leggen tussen de voorafbetaalde kaart en het product dat reeds gekocht is door de eindgebruiker. <u>De betrokken onderneming vergewist zich ervan, door technische en operationele maatregelen in te stellen, dat de persoon die de uitbreiding van het product vraagt, daadwerkelijk de voor dat product geïdentificeerde persoon is. Dit kan bijvoorbeeld worden gedaan via de voorlegging van een identiteitsstuk of aan de hand van het identificatienummer en een wachtwoord.</u> De persoon die de houder is van het product waarmee de voorafbetaalde kaart geassocieerd is, moet dezelfde persoon zijn als diegene die de activering van de voorafbetaalde kaart vraagt. Deze methode mag dus niet worden gebruikt als een kind de activering van de voorafbetaalde kaart vraagt en daarbij een beroep doet op een ander product waarop een ouder heeft ingetekend."[14] *(eigen onderlijning)*

[14] Verslag aan de Koning bij Koninklijk Besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart, *BS* 7 december 2016. (eigen onderstreping door de Geschillenkamer)

49. Uit het bovenstaande blijkt derhalve duidelijk en ondubbelzinnig dat de betrokken onderneming (*in casu* verweerder) zelfs een wettelijke plicht heeft om in het geval van productmigratie, zekerheid te verkrijgen omtrent de identiteit van de persoon die verzoekt om de migratie. Voorgaande dient ertoe zekerheid te verkrijgen over of het daadwerkelijk degene is die voor dat product is geïdentificeerd. Uit de memorie van toelichting blijkt bovendien dat de verificatie enkel kan plaatsvinden na voorleggen van een identiteitsstuk ofwel aan de hand van een identificatienummer en een wachtwoord.

50. Gezien de duidelijke en onmiskenbare bewoordingen van de wetgever in bovengenoemde regelgeving waarin volgens de Geschillenkamer geen ruimte wordt overgelaten tot een andere interpretatie, had er een verificatie van de identiteit moeten plaatsvinden. De Geschillenkamer oordeelt dat verweerder wel degelijk had moeten overgaan tot het controleren van de identiteit van de persoon die verzocht om migratie van de simkaart. De wetgever schrijft immers uitdrukkelijk voor dat deze controle dient te geschieden op basis van de identiteitskaart of identificatienummer en wachtwoord.

51. Verweerder mocht derhalve niet volstaan met het vragen naar het simkaartnummer en het telefoonnummer. Verweerder had immers de beschikking over de identiteitskaart van de derde, maar heeft nagelaten de persoonsgegevens te vergelijken met die van de houder van het gsm-nummer, *in casu* klager.

52. Door het uitvoeren van een verificatie zou snel genoeg blijken dat het om twee verschillende personen ging. Verweerder heeft nagelaten om een dergelijke weinig moeite vereisende verificatie uit te voeren, terwijl juist verweerder als telecomoperator zich bewust moest zijn van de enorme gevolgen die een dergelijke nalatigheid met zich mee zou kunnen brengen. Verweerder heeft hierdoor bewust nagelaten uitvoering te geven aan een wettelijke verplichting, namelijk die van artikel 18 § 1 Koninklijk Besluit ter uitvoering van de Wet Telecommunicatie. De Geschillenkamer komt tot de vaststelling dat er niet enkel sprake was van een toerekenbare tekortkoming maar ook van een schending van artikel 18 § 1 van het KB welke duidelijk voorschrijft dat een controle dient plaats te vinden bij productmigratie.

53. Verweerder heeft gedurende de procedure steeds opgeworpen dat productmigratie moest worden aangemerkt als commercieel doeleinde en dat het daarom verboden was om een verificatie van de identiteit uit te voeren. Uit artikel 18 §1 van het KB blijkt echter dat de wetgever productmigratie niet aanmerkt als commercieel doeleinde en juist voorschrijft dat er een verificatie van de identiteit dient plaats te vinden. Derhalve faalt het argument van verweerder.

54. De Geschillenkamer oordeelde in haar primaire beslissing onder andere dat verweerder de verwerking in overeenstemming diende te brengen met de artikelen 5.1.f, 5.2, 24 en 32 AVG. Verweerder heeft uitvoering gegeven aan dit bevel, door een bijkomende procedure aan te nemen om de identiteit van de klant bij productmigratie te verifiëren. Daarover stelt verweerder

in haar conclusie echter dat dit gebeurde op risico dat verweerder door het BIPT of door een rechtbank kan worden teruggefloten in verband met het gebruiken van de identificatiegegevens voor commerciële doeleinden, hetgeen uitdrukkelijk door artikel 126 van de WEC zou zijn verboden.

55. De Geschillenkamer concludeert dat een productmigratie volgens de geldende wetgeving niet als commercieel doeleinde kan worden beschouwd. Derhalve stelt zij nogmaals vast dat de artikelen 5 (1) (f), 5.2, 24 en 32 van de AVG zijn geschonden.

Tweede middel: Verweerder nam proactieve maatregelen conform artikel 5 (2) van de AVG teneinde de naleving van de voorschriften van de AVG, waaronder de technische en organisatorische maatregelen te waarborgen.

56. De verweerder voert als tweede middel aan dat er wel degelijk proactieve maatregelen werden getroffen teneinde de naleving van de voorschriften van de AVG - waaronder de technische en organisatorische maatregelen - te waarborgen. Verweerder heeft bij conclusie van antwoord onder andere de *Werkmethode Veiligheid* toegevoegd. Dit interne stuk voor de medewerkers omschrijft hoe er dient te worden omgegaan met persoonsgegevens van klanten en reikt handvatten aan om de vertrouwelijkheid van de gegevens binnen de organisatie van verweerder te waarborgen.

57. Op verschillende plaatsen in de *werkmethode* wordt erop gewezen dat een volledige identiteitscheck (naam, voornaam, telefoonnummer, als deze er is: klantnummer, geboortedatum, identiteitskaartnummer, adres, bedrag van de laatste factuur en waar en wanneer de activering is aangevraagd) vereist is voor "*alle vragen in het licht van contractwijziging, zoals; verandering van het tariefplan, verandering adres, P2P, PPP, activering of deactivering van een dienst, vraag om kopie van een factuur en vraag om vertrouwelijke informatie*".

58. *In casu* vroeg de derde die (later) beschikking kreeg over het telefoonnummer van klager, de omzetting van zijn prepaid-kaart naar een postpaid-abonnement. Hij vroeg derhalve om activering van een nieuwe dienst. Dit betekent dat verweerder ook volgens de eigen *werkmethode* had moeten vragen naar bijkomende gegevens met als doel het vaststellen van de identiteit van de persoon in kwestie. Door na te laten de identiteit van de derde met zekerheid vast te stellen, heeft verweerder verwijtbaar nalatig gehandeld.

59. Verweerder heeft daarnaast ook de documenten *Y Belgium overzicht van Technische en* Organisatorische *maatregelen en Group Security Standard* ingebracht in de procedure (zie punt 39 hierboven).

60. Volgens verweerder kan mede uit deze documenten worden afgeleid dat verweerder zich bekommert om te allen tijde de gepaste technische en organisatorische maatregelen te nemen om de persoonsgegevens van haar abonnees te beveiligen. De genomen maatregelen worden door haar ook ieder jaar geëvalueerd en, indien nodig, aangepast. Beide documenten bevatten algemene minimaal te implementeren beveiligingseisen. De Geschillenkamer kan op basis van deze documenten echter niet tot een ander oordeel komen dan dat verweerder in casu tekort is geschoten door de technische en organisatorische maatregelen onvoldoende ten uitvoer te brengen.

61. Verweerder stelt dat de inbreuk zeer beperkte gevolgen heeft gehad voor klager. De derde persoon kon volgens verweerder geen toegang krijgen tot de profielen van klager op verschillende platforms zoals WhatsApp en Paypal omdat die platforms de tweestapsverificatie zouden gebruiken teneinde te kunnen inloggen of aanmelden op hun profielen. De derde had volgens klager bovendien geen toegang tot alle communicatie van de klager die in het verleden had plaatsgevonden. Derhalve is er volgens verweerder op geen enkele manier sprake van schending van de privacy van klager. Er is enkel sprake van praktische ongemakken die klager zou ondervonden hebben.

62. De Geschillenkamer wijst er in dit verband op dat het - in tegenstelling tot het door verweerder beweerde - voor het gebruik van bijvoorbeeld de WhatsApp-applicatie in beginsel volstaat dat iemand beschikt over het telefoonnummer. De tweestapsverificatie die volgens verweerder dient te worden doorlopen moet via de WhatsApp-instellingen expliciet worden geactiveerd en staat niet standaard aan. De standaard beveiligingsinstelling is dus dat enkel het telefoonnummer volstaat voor het overnemen van het gebruik van de Whatsapp-applicatie. De gebruiker voert het telefoonnummer in via hetwelk hij de communicatie via de applicatie wenst te gebruiken en vervolgens wordt er een SMS-bericht verstuurd naar dat nummer. Nadat de code die in het SMS-bericht staat wordt ingevoerd, kan er direct worden gecommuniceerd via WhatsApp. Er is – indien de tweetrapsverificatie niet geactiveerd werd – dus niets anders nodig dan toegang tot het mobiele telefoonnummer waarnaar de verificatiecode wordt verstuurd.

63. Door te beschikken over een telefoonnummer, bestaat er bovendien een aanmerkelijke kans dat er inzage verkregen kan worden in verschillende soorten persoonsgegevens. Verschillende instanties - zoals bijvoorbeeld ziekenhuizen - doen herinneren aan afspraken middels het versturen van SMS -berichten. Bovendien zet het beschikken over een telefoonnummer van een ander de deur voor fraude en oplichting wagenwijd open, doordat er bijvoorbeeld gesprekken en berichten in naam van de benadeelde zouden kunnen worden gevoerd of gestuurd. De Geschillenkamer is het dus oneens met de stelling van verweerder dat er op geen enkele manier sprake zou zijn van schending van de privacy.

64. Het Hof van Justitie benadrukte het belang van telecomgegevens met de volgende bewoordingen in haar arrest Digital Rights Ireland van 8 april 2014: *"Uit deze gegevens, in hun*

geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren."[15] Niettegenstaande de derde *in casu* wellicht niet over alle in het arrest genoemde gegevens kon beschikken, is de Geschillenkamer van mening dat er door het beschikken over het telefoonnummer van de klager sprake was van een significant gevaar voor de schending van diens privacyrechten.

65. Verweerder stelt bij conclusie dat in principe enkel de gebruiker van een mobiel telefoonnummer het daaraan gekoppelde simkaartnummer zou mogen kennen. Het simkaartnummer wordt daarom gebruikt als verificatie dat de aanvrager weldegelijk de werkelijke gebruiker is van het telefoonnummer dat opgegeven wordt. De verkoper zou daarom in de winkel zowel het telefoonnummer als het simkaartnummer aan de derde hebben gevraagd en verkregen. De migratie is toen uitgevoerd en de derde heeft daarbij dus zijn eigen identificatiegegevens opgegeven, volgens verweerder. De identificatiegegevens van de derde werden volgens verweerder gecontroleerd door de identiteitskaartgegevens te vergelijken met de opgegeven naam, adres en woonplaats van de derde. Deze identiteitsgegevens werden volgens verweerder echter niet vergeleken met de identiteitsgegevens van de prepaid-klant aan wie het simkaartnummer en gsm-nummer eerst was toegekend, namelijk klager. Laatstgenoemde controle gebeurde volgens verweerder niet omdat identiteitsgegevens niet mogen worden gebruikt voor commerciële toepassingen op basis van de Wet Elektronische Communicatie[16] en het Verslag aan de Koning bij het Koninklijk besluit dat uitvoering aan deze wet geeft,[17] zoals uiteengezet in randnummer 42 e.v. hierboven.

66. Verweerder vindt het onbegrijpelijk dat de derde het simkaartnummer te weten kon komen. Volgens verweerder kan het simkaartnummer enkel worden achterhaald via de systemen van verweerder waar deze is opgeslagen of indien deze zijn medegedeeld door klager zelf. Teneinde zowel het telefoonnummer als het simkaartnummer te verkrijgen zou de derde – volgens verweerder - ofwel de medewerking van klager gehad hebben ofwel die van een Y medewerker. Volgens verweerder is de combinatie tussen simkaart en telefoonnummer uniek, waardoor de werkwijze om de combinatie telefoonnummer-simkaartnummer te gebruiken passend is om de identiteit van de gebruiker te verifiëren. Indien enkel zou gebruik gemaakt worden van het telefoonnummer om de identiteit van de gebruiker te verifiëren voor de migratie, zou dit volgens verweerder wel kunnen wijzen op gebrekkige technische en organisatorische maatregelen. De

[15] Hof van Justitie EU, Digital Rights Ireland en Seitlinger e.a, Gevoegde zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 , r.o. 27.

[16] Artikel 127 juncto artikel 126 § 2,7° *Wet betreffende de elektronische communicatie* van 13 juni 2005, in werking getreden op 30 juni 2005.

[17] Verslag aan de Koning bij Koninklijk Besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart, *BS* 7 december 2016.

combinatie van telefoonnummer en simkaartnummer kan volgens verweerder worden gelijkgesteld met de combinatie van e-mailadres en paswoord. Ook in deze combinatie bestaat de verificatie uit een element dat publiek is en een element dat enkel de eigenaar kan kennen.

67. De Geschillenkamer wijst op de verklaring van verweerder dat:

- medewerkers verplicht het simkaartnummer dienden op te vragen bij de klant en deze dienden in te voeren om een migratie te bewerkstelligen van prepaid naar postpaid;
- er destijds geen mogelijkheid voor de medewerker bestond om aan de hand van het gsm-nummer het simkaartnummer op te vragen in de databank.

Derhalve blijft de vraag hoe de derde aan de combinatie gsm-nummer – simkaartnummer is gekomen. De verweerder heeft dit in ieder geval niet ten overstaan van de Geschillenkamer kunnen aantonen, zoals vereist door de artikelen 5.2 en 24 AVG.

68. Verweerder legt een eerdere melding d.d. 11 maart 2019 aan de Gegevensbeschermingsautoriteit van een soortgelijk gegevenslek over.[18] Daarbij wordt vermeld dat een andere reden van het *in casu* geen melding maken van het lek het volgende was : *'De Gegevensbeschermingsautoriteit heeft dit dossier niet verder opgevolgd, wat blijk geeft van de beperkte gewichtigheid die de Gegevensbeschermingsautoriteit aan dergelijke (kleine) gegevenslek geeft. Om die reden werd het vermoeden van concluante dat er geen meldingsplicht zou zijn in onderhavig geval bevestigd."* De Geschillenkamer wijst hierbij op de verantwoordingsplicht van verweerder welke voortvloeit uit artikel 5.2 en artikel 24 AVG waarbij het aan de verweerder is om aan te tonen dat zij tevens handelt conform artikel 5.1.f AVG namelijk: *"door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid")."* De bewering dat een eerdere melding niet werd behandeld door de Gegevensbeschermingsautoriteit, doet niet af aan de verantwoordingsverplichting.

69. De Geschillenkamer wijst er eens te meer op dat de verantwoordingsplicht ingevolge de artikelen 5, lid 2, artikel 24 en artikel 32 AVG met zich meebrengt dat de verwerkingsverantwoordelijke de nodige technische en organisatorische maatregelen neemt, teneinde ervoor zorg te dragen dat de verwerking in overeenstemming is met de AVG. De voorgaande verplichting behoort tot het degelijk invullen van de verantwoordelijkheid van verweerder ingevolge artikel 5, lid 2, 24 en 32 AVG. De Geschillenkamer wijst er op dat de verantwoordingsplicht van artikel 5 lid 2 en artikel 24 AVG één van de centrale pijlers van de AVG vormt. Dit houdt in dat op de

[18] Als stuk 5 bij haar conclusies.

verwerkingsverantwoordelijke de verplichting rust tot, enerzijds, het nemen van proactieve maatregelen teneinde de naleving van de voorschriften van de AVG te waarborgen en, anderzijds, het kunnen aantonen dat hij dergelijke maatregelen heeft getroffen.

70. De Groep 29 heeft in het Advies betreffende het "verantwoordingsbeginsel" te kennen gegeven dat twee aspecten van belang zijn bij de interpretatie van dit beginsel:

(i) "*de noodzaak voor een voor de verwerking verantwoordelijke om passende en doeltreffende maatregelen te nemen teneinde de beginselen voor gegevensbescherming ten uitvoer te leggen; en*

(ii) *de noodzaak om op verzoek te kunnen aantonen dat er passende en doeltreffende maatregelen zijn genomen. De voor de verwerking verantwoordelijke moet derhalve bewijs kunnen overleggen van (i) hierboven*".[19]

71. De Geschillenkamer is gezien bovenstaande overwegingen van oordeel dat verweerder **inbreuk heeft gepleegd op de artikelen 5.1.f, 5.2, 24 en 32 AVG** door onvoldoende technische en organisatorische maatregelen te treffen om de verwerking van persoonsgegevens in overeenstemming met de relevante wet- en regelgeving te laten verlopen.

Gegevenslek

72. Artikel 33 lid 1 AVG bepaalt : "*Indien een inbreuk in verband met persoonsgegevens heeft* plaatsgevonden*, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.*"

73. Verweerder stelt in haar conclusies dat er geen verplichting bestond om het gegevenslek door te geven aan de Gegevensbeschermingsautoriteit. De reden daarvan is volgens verweerder het feit dat het gegevenslek één betrokkene betrof, het van zeer korte duur was en er volgens verweerder geen sprake was van gevoelige gegevens. Wat betreft het voorgaande wijst de Geschillenkamer op het hierboven overwogene, namelijk dat het aannemelijk kan worden geacht dat er bijvoorbeeld SMS-berichten worden ontvangen welke bijzondere persoonsgegevens zouden kunnen bevatten.

[19] Advies 3/2010 over het "verantwoordingsbeginsel" vastgesteld op 13 juli 2010 door de Groep 29, p. 10 – 14 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_nl.pdf.

74. Bij de beoordeling van de vraag of een inbreuk een waarschijnlijk hoog risico vormt voor de rechten en vrijheden van natuurlijke personen dient volgens de Richtsnoeren van de Groep 29 rekening gehouden te worden met het antwoord op de vraag of de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor de personen wier gegevens het voorwerp van de inbreuk zijn. Voorbeelden van dergelijke schade zijn discriminatie, identiteitsdiefstal of -fraude, financieel verlies en reputatieschade.[20] Door het telefoonnummer van klager toe te kennen aan een derde, is klager blootgesteld aan het gevaar van het uitvoeren van frauduleuze handelingen onder zijn naam, door gebruik te maken van zijn telefoonnummer. Ook bestaat – anders dan verweerder lijkt te stellen - een risico dat gevoelige gegevens (zoals gezondheidsgegevens) in handen komen van derden. Verweerder stelt dat er geen meldplicht bestond voor haar, onder andere omdat het gaat om een inbreuk van gegevens van één enkel persoon. De Geschillenkamer wijst erop dat een inbreuk echter zelfs voor één persoon ernstige gevolgen kan hebben, geheel afhankelijk van de aard van de persoonsgegevens en de context waarin deze zijn gecompromitteerd. Ook hier komt het erop aan te kijken naar de waarschijnlijkheid en ernst van de gevolgen.[21] Bovendien betreft het hier een risico van structurele aard waar mogelijk alle gebruikers van prepaidkaarten aan blootgesteld kunnen worden. Het kan niet worden uitgesloten dat er andere gevallen zijn waar de Geschillenkamer niet van op de hoogte is.

75. De Geschillenkamer is van oordeel dat verweerder er in onderhavig geval niet in is geslaagd aan te tonen dat er voldoende proactieve maatregelen waren genomen om naleving van de AVG te waarborgen. De medewerkers van verweerder hebben allereerst nagelaten een verificatie uit te voeren tussen de identiteiten van de derde en die van klager en Y heeft vervolgens nagelaten om het gegevenslek te melden aan de Gegevensbeschermingsautoriteit. Verweerder heeft geen stukken bijgebracht waaruit blijkt dat is voldaan aan de documentatieplicht die op verweerder rustte. Het enige document dat door verweerder werd bijgebracht betreffende een gegevenslek, was een melding van een ander gegevenslek door verweerder aan de Gegevensbeschermingsautoriteit daterend uit het jaar 2019. Uit de stukken van het dossier, hetgeen ter zitting naar voren is gebracht en het feit dat verweerder geen documentatie van het gegevenslek heeft ingebracht, blijkt dat verweerder evenmin voldoet aan de plicht van artikel 33 lid 5 AVG waarin is bepaald:

> *'De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die*

[20] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens verordening 2016/679, *wp250rev.01,* Werkgroep 29, p.26.

[21] Idem, p. 30

documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren."

76. De Geschillenkamer wees er reeds eerder in beslissing 2020/22 op dat: "*de verantwoordingsplicht toegepast op gegevenslekken inhoudt dat op een verwerkingsverantwoordelijke met betrekking tot deze gegevenslekken niet enkel de verplichting rust deze desgevallend overeenkomstig artikelen 33 en 34 AVG te melden aan de toezichthoudende autoriteit en de betrokkenen, doch dat deze* eveneens *te allen tijde moet kunnen aantonen dat hij de nodige maatregelen heeft genomen om te kunnen voldoen aan deze verplichting"*[22] De Geschillenkamer is van oordeel dat zulks in onderhavig geval niet is aangetoond.

77. In een niet-uitputtende lijst die verwerkingsverantwoordelijken kunnen treffen om aan de verantwoordingsverplichting te voldoen wordt door de Groep 29 verwezen naar onder andere de volgende te nemen maatregelen: het ten uitvoer leggen van en toezicht houden op controleprocedures om te waarborgen dat alle maatregelen niet alleen op papier bestaan maar ook ten uitvoer worden gelegd en in de praktijk functioneren, het vaststellen van interne procedures, het opstellen van een schriftelijk en bindend beleid betreffende gegevensbescherming, het ontwikkelen van interne procedures voor het doeltreffend beheren en rapporteren van inbreuken op de beveiliging.

78. De Geschillenkamer wijst bovendien op een formulier dat bij de conclusie is gevoegd en waarin melding werd gemaakt van een soortgelijk gegevenslek, namelijk het telefoonnummer van een klant die naar een andere operator was overgestapt. Dit telefoonnummer werd ten onrechte als vrij gezien en aan een nieuwe klant toegekend. In het formulier heeft verweerder de vraag "*Wat is de hoogte van de graad of het niveau van de ernst van het gegevenslek voor betrokkenen bij het beoordelen van de risico's voor de rechten en vrijheden van betrokkenen ?*", notabene beantwoord met *'kritisch"* gegevenslek. Hieruit blijkt volgens de Geschillenkamer duidelijk dat ook verweerder de ernst van een dergelijk gegevenslek wel degelijk inziet.

79. De Geschillenkamer stelt derhalve **inbreuken vast op artikel 33 leden 1 en 5 AVG**. De Geschillenkamer wijst erop, dat er in hoofde van de verwerkingsverantwoordelijke een verplichting is om elk gegevenslek, ongeacht of dit risicovol is of niet, te documenteren teneinde informatie te kunnen verstrekken aan de GBA. De verwerking van persoonsgegevens is immers een kernactiviteit van verweerder. Persoonsgegevens kunnen bovendien een grote mate van

[22] Beslissing 22/2020 van 8 mei 2020 van de Geschillenkamer, p.12

gevoeligheid hebben voor betrokkenen, onder meer omdat ze een regelmatige en stelselmatige observatie mogelijk maken.[23]

80. Verweerder brengt bij conclusie een document *Data Breach Assessment* bij. In dit document is het gegevenslek gedocumenteerd op 15 april 2020, 7 maanden nadat het gegevenslek plaatsvond. In het document valt onder andere het volgende te lezen*:*

'Het incident gaf een derde partij toegang tot de communicatie-inhoud van de klant van een pre-paid kaart gedurende 3,25 dagen. De derde had niet de bedoeling de gegevens te gebruiken, te misbruiken of te verspreiden. De gegevens waren derhalve niet publiekelijk beschikbaar op het internet.
De theoretische impact van de inbreuk is dus zeer groot, aangezien het om de inhoud van de communicatie gaat, en hoewel de waarschijnlijkheid dat de inbreuk gevolgen heeft voor de betrokkene laag is, is het resultaat een algemeen zeer hoog risico.

Maar op basis van de informatie die van de betrokkene is ontvangen, was de met een derde gedeelde communicatie-inhoud waarschijnlijk beperkt tot tweestapsauthenticatiecodes en dit gedurende een periode van 3,5 dagen. Deze tweestapsauthenticatiecodes kunnen niet worden gebruikt door de derde partij die geen toegang heeft tot de inloggegevens van de betrokkene. De gevolgen voor de betrokkene zijn dus beperkt en het risico is bijgesteld tot een laag risico."

81. Uit de hierboven geciteerde tekst blijkt nogmaals dat verweerder zich wel degelijk bewust was van het feit dat er *in casu* sprake was van een "zeer hoog risico" aangezien het ging om inhoud van telecommunicatie. Het risico werd terug bijgesteld tot "laag" nadat verweerder te weten was gekomen dat de gedeelde inhoud waarschijnlijk was beperkt tot tweestapsauthenticatiecodes. Aangezien derden geen toegang konden hebben tot de inloggegevens van klager, werd het niveau dus bijgesteld. Zoals de Geschillenkamer reeds eerder opmerkte vormden niet enkel de applicaties die een tweestapsauthenticatie behoeven een risico voor de klager, maar ook zijn telefoon en sms- verkeer werd blootgesteld aan grote risico's op onder andere fraude die gepleegd had kunnen worden onder zijn naam. De Geschillenkamer oordeelt dat er wel sprake was van een hoog risico.

82. Verweerder is van mening dat er geen plicht rustte op haar om de klager van het gegevenslek op de hoogte te brengen. Verweerder heeft derhalve nagelaten om nadat hij zelf op de hoogte raakte, klager middels een mededeling op de hoogte te stellen van de toekenning van het telefoonnummer aan een derde. De Geschillenkamer oordeelt dat de melding aan de betrokkene

[23] Beslissing 18/2020 van 28 april 2020 van de Geschillenkamer

in dit specifieke geval achterwege mocht blijven gezien de bijzondere omstandigheid van dit geval waarbij de betrokkene reeds op de hoogte was van het gegevenslek. De Geschillenkamer oordeelt derhalve dat er **geen inbreuk is vastgesteld op artikel 34 AVG.**

83. De Geschillenkamer wijst op onderstaand voorbeeld welke het belang van de mededeling van een gegevenslek aan de betrokkenen en de bevoegde autoriteit, eens te meer duidelijk maakt. Het betreft een voorbeeld in de recentelijk gepubliceerde "*Guideline on Examples regarding Data Breach Notification*" van de EDPB[24] waarin het contactcentrum van een telecommunicatie-bedrijf wordt gebeld door een persoon die zegt een klant te zijn en vraagt een wijziging van zijn e-mailadres door te voeren zodat de rekeningen voortaan naar dat nieuwe e-mailadres worden gestuurd. De beller geeft de juiste persoonsgegevens van de klant door waarna de facturen voortaan naar het nieuwe e-mailadres worden gestuurd. Wanneer de eigenlijke klant belt met het bedrijf om te vragen waarom hij geen facturen meer ontvangt, beseft het bedrijf dat de facturen naar een ander worden gestuurd.

84. De EDPB overweegt het volgende omtrent bovenstaand voorbeeld :

'This case serves as an example on the importance of prior measures. The breach, from a risk aspect, presents a high level of risk, as billing data can give information about the data subject's private life (e.g.habits, contacts)and could lead to material damage (e.g. stalking, risk to physical integrity). The personal data obtained during this attack can also be used in order to facilitate account takeover in this organisation or exploit further authentication measures in other organisations. Considering these risks, the 'appropriate" authentication measure should meet a high bar, depending on what personal data can be processed as a result of authentication.

As a result, both a notification to the SA and a communication to the data subject are needed from the controller. The prior client validation process is clearly to be refined in light of this case. The methods used for authentication were not sufficient. The malicious party was able to pretend to be the intended user by the use of publicly available information and information that they otherwise had access to. The use of this type of static knowledge-based authentication (where the answer does not change, and where the information is not 'secret" such as would be the case with a password) is not recommended."[25]

---

[24] EDPB *Guideline on Examples regarding Data Breach Notification,* 01/2021, gepubliceerd op www.edpb.europa.eu.

[25] EDPB *Guideline on Examples regarding Data Breach Notification,* 01/2021, p.30

Onderlijning door de Geschillenkamer

Vrije vertaling: Deze casus dient als voorbeeld over het belang van het treffen van voorafgaande maatregelen. De inbreuk vormt vanuit risicoaspect een hoog risico, aangezien factureringsgegevens informatie kunnen geven over het privéleven van de betrokkene (bijv. gewoonten, contacten) en kunnen leiden tot materiële schade (bijv. stalking, risico voor fysieke integriteit). De persoonsgegevens die bij deze aanval worden verkregen, kunnen ook worden gebruikt om accountovername in deze organisatie te vergemakkelijken of om verdere authenticatiemaatregelen bij andere organisaties te benutten. Gezien deze risico's moet de 'passende' authenticatiemaatregel aan eisen voldoen en afhankelijk daarvan kan worden bepaald van welke persoonsgegevens kunnen worden verwerkt.

85. De melding van inbreuken moet worden gezien als een manier om de naleving van de regels inzake de bescherming van persoonsgegevens te verbeteren. Derhalve is er volgens de Geschillenkamer geenszins sprake van “kennisgevingsmoeheid” zoals door verweerder wordt aangehaald. De Groep 29 stelt daarover immers :

‘Verwerkingsverantwoordelijken moeten onthouden dat de melding van een inbreuk aan de toezichthoudende autoriteit verplicht is, tenzij het onwaarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van natuurlijke personen inhoudt. Als het waarschijnlijk is dat een inbreuk resulteert in een hoog risico voor de rechten en vrijheden van natuurlijke personen, moeten natuurlijke personen ook worden geïnformeerd. De drempel voor het meedelen van een inbreuk aan personen ligt dus hoger dan die voor het melden van een inbreuk aan de toezichthoudende autoriteiten, en dus hoeven niet alle inbreuken aan personen te worden gemeld, waardoor ze worden beschermd tegen onnodige kennisgevingsmoeheid.”[26]

Wanneer er een inbreuk in verband met persoonsgegevens plaatsvindt of heeft plaatsgevonden, kan dit leiden tot materiële of immateriële schade aan natuurlijke personen of enige andere economische, lichamelijke of sociale schade voor de betrokken persoon. Derhalve dient de verwerkingsverantwoordelijke in de regel zodra hij kennis neemt van een inbreuk in verband met persoonsgegevens met een risico voor de rechten en vrijheden van betrokkenen, de toezichthoudende autoriteit zonder onnodige vertraging en, indien mogelijk, binnen 72 uur op de hoogte te stellen van de inbreuk. Daardoor kan de toezichthoudende autoriteit haar taken en bevoegdheden, zoals vastgelegd in de AVG, naar behoren uitvoeren.

Reactie op boeteformulier en recht van verdediging

86. Verweerder heeft op 31 mei 2022 gereageerd op het voornemen tot opleggen van een geldboete.

87. De verweerder herhaalt daarin dat de samenstelling van de Geschillenkamer volgens hem onregelmatig is, en de procedure evenzeer, aangezien de voorzitter is blijven zetelen niettegenstaande de beslissing van het Marktenhof. Volgens verweerder is niet bewezen dat er

Hierdoor is zowel een melding aan de toezichthoudende autoriteit als een mededeling aan de betrokkene nodig door de verwerkingsverantwoordelijke. Het voorafgaande klantvalidatieproces moet in het licht van dit geval duidelijk worden verfijnd. De methoden die werden gebruikt voor authenticatie waren niet voldoende. Een kwaadwillende had zich kunnen voordoen als de beoogde gebruiker door gebruik te maken van openbaar beschikbare informatie en informatie waartoe zij op andere wijze toegang tot hadden. Het gebruik van dit type statische, op kennis gebaseerde authenticatie (waarbij het antwoord niet verandert en waar de informatie niet "geheim" is zoals het geval zou zijn met een wachtwoord) wordt niet aanbevolen.”

[26] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, Werkgroep artikel 29, WP25 0.rev.01

sprake was van een gegevenslek en berust de vaststelling van het bestaan van een gegevenslek louter op vermoedens. Er is geen enkel bewijs aangeleverd door klager van het bestaan van een gegevenslek. De verweerder is van oordeel dat hij voldoende technische en organisatorische maatregelen trof teneinde een voorval als *in casu* te voorkomen. Verweerder stelt herhaaldelijk de regels van de Wet Elektronische Communicatie (WEC) te hebben nageleefd en geeft te kennen dat voornoemde wet het controleren en verifiëren van de identiteit in het kader van commerciële doeleinden verbiedt. De migratie van een simkaart dient volgens verweerder aangemerkt te worden als een commercieel doeleinde. Verweerder geeft te kennen dat het door hen gehanteerde beveiligingsbeleid in een eerdere beslissing van de Geschillenkamer als behoorlijk werd aanzien. Verweerder wijst er nogmaals op dat er geen sprake was van een meldplicht van het gegevenslek aan de Gegevensbeschermingsautoriteit aangezien het om 1 betrokkene ging, het gegevenslek van korte duur was en er geen sprake zou zijn van gevoelige persoonsgegevens.

88. Verweerder kan zich niet vinden in de vaststelling van de Geschillenkamer dat er sprake is geweest van een *'disproportionele mate van nalatigheid"* aangezien verweerder er alles aan doet om persoonsgegevens zo goed mogelijk te beveiligen. Bovendien was er geen sprake van opzet of kwade wil zijdens verweerder. Verweerder is van mening dat de voorgenomen geldboete van 20.000 EUR niet in verhouding staat tot de inbreuken die zijn vastgesteld. Het opleggen van een boete staat volgens verweerder in schril contract met eerdere beslissingen van de Geschillenkamer waarbij dergelijke gevallen met 1 betrokkene en een beperkte maatschappelijke impact zouden zijn geseponeerd. Verweerder stelt zelf slachtoffer te zijn van een malafide persoon die de persoonsgegevens van de klager heeft weten te bemachtigen. Tevens is er geen sprake van eerdere inbreuken gepleegd door verweerder. Dit geheel maakt het opleggen van een geldboete van 20.000 EUR onredelijk. Verweerder vindt een waarschuwing meer op zijn plaats. Mocht de Geschillenkamer toch een geldboete willen opleggen, verzoekt verweerder de Geschillenkamer de boete te beperken tot een bedrag van 5.000 EUR. Wat betreft de jaarcijfers geeft verweerder te kennen dat er een lichte afwijking is met jaarcijfers die door de Geschillenkamer werden voorgelegd in het sanctieformulier; het juiste bedrag is 1.3XX.XXX.XXX EUR in plaats van 1.2XX.XXX.XXX EUR.

89. De Geschillenkamer is van oordeel dat alle door verweerder aangevoerde argumenten in het sanctieformulier reeds werden behandeld in onderhavige beslissing en in aanmerking werden genomen bij de vaststelling van de administratieve geldboete overeenkomstig artikel 83.2 AVG. De Geschillenkamer heeft in de beslissing immers uiteengezet dat het gegevenslek te wijten is aan nalatigheid aan de kant van verweerder. Verweerder had volgens de Geschillenkamer immers zowel op basis van de WEC alsook volgens interne regelgeving de identificatiegegevens moeten verifiëren om er zeker van te zijn dat de persoon die in de winkel stond ook daadwerkelijk

de houder van het telefoonnummer was. Dit heeft verweerder nagelaten. Bovendien is nagelaten daarvan een melding te doen aan de Gegevensbeschermingsautoriteit. De Geschillenkamer deelt de visie van verweerder niet waar deze stelt dat er geen sprake is van bewijs waaruit blijkt dat derden kennis hebben genomen van de persoonsgegevens waardoor het bestaan van een gegevenslek niet kan worden aangetoond. Zoals de Geschillenkamer onder punt 63 aangaf, bestond er een merkelijke kans dat de derde inzage had in (gevoelige) persoonsgegevens van klager; immers deze derde had gedurende vier dagen de beschikking over het telefoonnummer. Derhalve kan niet worden uitgesloten dat inzage door die derde in de persoonsgegevens van klager heeft plaatsgevonden.

90. Het betreft *in casu* een verwerkingsverantwoordelijke die dagelijks massaal gegevens verwerkt waarvan kan en mag worden verwacht dat hij de juiste technische en organisatorische maatregelen treft teneinde de bescherming van persoonsgegevens te garanderen. Gezien voorstaande is de Geschillenkamer van oordeel dat een boete van 20.000 EUR kan worden aangemerkt als een zeer geringe boete in verhouding tot de vastgestelde inbreuken en de omzet die blijkt uit de jaarcijfers van verweerder.

91. Tot slot wijst de Geschillenkamer erop dat op haar geen verplichting rust, noch op basis van de AVG of de WOG, noch op basis van rechtspraak van het Marktenhof, om de motivering van de onderhavige beslissing voorafgaand aan het nemen van de betrokken beslissing aan de tegenspraak van de verwerende partijen te onderwerpen, het sanctieformulier dient er enkel toe de mogelijkheid tot tegenspraak op de voorgenomen geldboete te bieden.

3. Inbreuken op de AVG

92. De Geschillenkamer acht inbreuken op de volgende bepalingen door de verweerder bewezen:

    a. **Artikel 5.1.f, 5.2, 24 en 32 AVG**, gezien verweerder onvoldoende voorzorgsmaatregelen nam om het gegevenslek te voorkomen;
    b. **artikel 33.1 en 33.5 AVG**, gezien verweerder geen melding maakte van het gegevenslek aan de GBA.

93. De Geschillenkamer acht het passend om een administratieve geldboete op te leggen ten bedrage van 20.000 EUR (artikel 83, lid 2 AVG; artikel 100, §1, 13° WOG en artikel 101 WOG).

94. Rekening houdend met artikel 83 AVG en de rechtspraak[27] van het Marktenhof, motiveert de Geschillenkamer het opleggen van een administratieve geldboete *in concreto*:

[27] Hof van Beroep Brussel (sectie Marktenhof), *X t. GBA,* Arrest 2020/1471 van 19 februari 2020.

a.) De ernst van de inbreuk: de Geschillenkamer stelt vast dat het gegevenslek onder andere te wijten is aan nalatigheid aan de kant van verweerder. Bovendien heeft verweerder nagelaten het lek te melden aan de Gegevensbeschermingsautoriteit en te kennen gegeven dat *in casu* geen sprake is van een waarschijnlijk hoog risico voor de rechten en plichten van klager waardoor er geen meldplicht zou bestaan voor verweerder. Het feit dat het *in casu* gaat om telecomgegevens waaruit precieze gegevens omtrent het privéleven van een persoon kunnen worden ontleend alsook het potentieel gevaar op het plegen van frauduleuze handelingen in naam van die persoon maken dat er sprake is van een ernstige inbreuk.

b.) De duur van de inbreuk: de inbreuk heeft vier dagen geduurd, wat een aanzienlijke termijn is in het licht van het hiervoor geduide potentieel gevaar.

c.) De op te leggen boete is dermate afschrikwekkend om dergelijke inbreuken in de toekomst te voorkomen. De Geschillenkamer herhaalt in deze context dat een boete van 20.000 EUR kan worden aangemerkt als een zeer geringe boete in verhouding tot de vastgestelde inbreuken en de omzet die blijkt uit de jaarcijfers van verweerder.

95. De Geschillenkamer wijst erop dat de andere criteria van art. 83.2. AVG in dit geval niet van aard zijn dat zij leiden tot een andere administratieve geldboete dan die welke de Geschillenkamer in het kader van deze beslissing heeft vastgesteld.

96. Ten overvloede wijst de Geschillenkamer nog op de richtsnoeren omtrent de berekening van administratieve boetes (Guidelines 04/2022 on the calculation of administrative fines under the GDPR) die de EDPB op 16 mei 2022 op haar website heeft gepubliceerd, ter consultatie. Aangezien deze richtsnoeren nog niet definitief zijn, heeft de Geschillenkamer besloten deze nog niet in aanmerking te nemen voor het bepalen van de hoogte van de boete in de onderhavige procedure.

97. Verweerder heeft in haar reactie op het voornemen tot opleggen van een boete bezwaar gemaakt tegen de hoogte van de voorgenomen geldboete. Uit dit dossier is volgens de Geschillenkamer echter gebleken dat er sprake was van onzorgvuldigheid en nalatigheid naar bescherming van persoonsgegevens van betrokkene toe. Het verwerken van persoonsgegevens maakt immers een kernactiviteit uit van de verweerder waardoor het van doorslaggevend belang is dat de persoonsgegevens worden verwerkt conform de AVG.

98. De feiten, omstandigheden en vastgestelde inbreuken rechtvaardigen derhalve een boete die tegemoetkomt aan de nood om een voldoende afschrikwekkende werking te hebben, waarbij de verweerder voldoende sterk wordt gesanctioneerd, opdat praktijken met dergelijke inbreuken niet zouden worden herhaald.

99. 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 partijen rechtstreeks worden bekendgemaakt.

OM DEZE REDENEN,

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

- op grond van artikel 83 AVG en artikelen 100, 13° en 101 WOG een administratieve geldboete **van 20.000 EUR** op te leggen aan de verweerder wegens de inbreuken op de artikelen 5.1.f, 5.2, 24, 32, 33.1 en 33.5 AVG.

Tegen deze beslissing kan op grond van art. 108, § 1 WOG, beroep worden aangetekend binnen een termijn van dertig dagen, vanaf de kennisgeving, bij het Marktenhof, met de Gegevensbeschermingsautoriteit als verweerder.

(Get). Hielke Hijmans
Voorzitter van de Geschillenkamer