Autorité de protection des données
Gegevensbeschermingsautoriteit

Geschillenkamer

Beslissing ten gronde 05/2021 van 22 januari 2021

deze beslissing werd ingetrokken bij beslissing 61/2021 van 19 mei 2021

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 Jelle Stassijns en Frank De Smet, 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,* 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,

- de verweerder: Y

1. Feiten en procedure

1. Klager dient 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 houdt 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.

2. Aangezien de klacht is gericht tegen Y met hoofdkantoor in lidstaat Z, heeft de Gegevensbeschermingsautoriteit contact opgenomen met de toezichthouder in deze lidstaat teneinde na te gaan of de klacht al dan niet als grensoverschrijdend diende te worden beschouwd. Die communicatie heeft ertoe geleid om de klacht en de gegevensverwerking te behandelen volgens de nationale procedure van de Belgische gegevensbeschermingsautoriteit (art. 56.2 AVG)[1] met Y als verweerder.

3. Op 15 april 2020 heeft de Geschillenkamer beslist dat de klacht gereed is 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.

4. Bij brief van 20 april 2020 hebben de raadslieden van verweerder zich gesteld in het dossier, kopie van het dossier opgevraagd en te kennen gegeven gehoord te willen worden op een hoorzitting op grond van artikel 98, 2° WOG.

5. Op 27 mei 2020 heeft verweerder een conclusie van antwoord neergelegd.

6. Zowel klager als verweerder hebben geen gebruik gemaakt van de mogelijkheid een conclusie van repliek in te dienen. Klager wenste geen gebruik te maken van de mogelijkheid om gehoord te worden.

[1] Artikel 56.2 luidt: In afwijking van lid 1 is elke toezichthoudende autoriteit competent een bij haar ingediende klacht of een eventuele inbreuk op deze verordening te behandelen indien het onderwerp van die zaak alleen verband houdt met een vestiging in haar lidstaat of alleen voor betrokkenen in haar lidstaat wezenlijke gevolgen heeft.

7. Op 9 november 2020 wordt de verweerder overeenkomstig artikel 53 van het reglement van interne orde gehoord door de Geschillenkamer.

8. Op 19 november 2020 wordt het proces-verbaal van de hoorzitting aan partijen voorgelegd. Hierop is door partijen niet gereageerd.

9. 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.

2. Rechtsgrond

Artikel 5.1.f AVG

1.Persoonsgegevens moeten :

f) 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").

Artikel 5.2 AVG

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen („verantwoordingsplicht").

Artikel 24 AVG

1. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd.

3. Het aansluiten bij goedgekeurde gedragscodes als bedoeld in artikel 40 of goedgekeurde certificeringsmechanismen als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de verplichtingen van de verwerkingsverantwoordelijke zijn nagekomen.

Artikel 32 AVG

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a) de pseudonimisering en versleuteling van persoonsgegevens;

b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen; d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

3. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.

4. De verwerkingsverantwoordelijke en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke verwerkt, tenzij hij daartoe Unierechtelijk of lidstaatrechtelijk is gehouden

Artikel 33 AVG

1.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.

2. De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.

3. In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld:

a)de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
b)de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
d)de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

4. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

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

Artikel 34.1 AVG

34.1 Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.

3. Motivering

3.1 Verweermiddelen en analyse Geschillenkamer

De gevolgde procedure

10. Verweerder heeft gereageerd op het voornemen tot opleggen van een geldboete. De reactie houdt onder andere in dat verweerder de mening is toegedaan dat de rechten van verdediging zijn geschonden door de Geschillenkamer. Volgens verweerder houden de door de Geschillenkamer vastgestelde inbreuken weinig tot geen verband met de initieel ingediende klacht door klager. Verweerder stelt dat de klager in zijn klacht enkel heeft aangegeven dat er sprake was van schending van zijn privacy zonder te benoemen om welke inbreuken het specifiek ging. Verweerder oordeelt dat het de taak van de Geschillenkamer was om die klacht juridisch te kwalificeren en van meet af aan kenbaar te maken aan verweerder. Verweerder stelt dat zij eerst op 7 december 2020, dus middels het voornemen tot oplegging van de boete, in kennis werd gesteld van de specifieke inbreuken en zich daardoor niet effectief heeft kunnen verdedigen tegen de tenlastelegging. Bovendien was het *in casu* volgens verweerder noodzakelijk dat de Geschillenkamer de Inspectiedienst zou hebben gevat. Dat is niet gebeurd en de Geschillenkamer heeft na sluiting van de debatten de feiten zelf juridisch gekwalificeerd, aldus verweerder.

11. De Geschillenkamer wenst in het algemeen de aandacht te vestigen op het feit dat het indienen van een klacht voor de betrokkenen wiens persoonsgegevens verwerkt worden, ongecompliceerd dient te zijn. De klachtenprocedure zoals voorzien in artikel 77 AVG en uitgewerkt in de WOG is bedoeld als een alternatief voor een beroep op de burgerlijke of administratieve rechter. Het klachtrecht bij de GBA moet gemakkelijk en laagdrempelig blijven voor de burger. Zo heeft de wetgever heeft bijvoorbeeld niet gewild dat partijen steeds door een advocaat worden bijgestaan.[2] Artikel 60 van de WOG stelt lage eisen aan de ontvankelijkheid van een klacht. Voor ontvankelijk verklaring is slechts vereist dat een klacht in één van de landstalen opgesteld moet zijn, een uiteenzetting moet bevatten van de feiten, alsook de nodige indicaties voor de identificatie van de verwerking waarop ze betrekking heeft, en moet vallen onder de bevoegdheid van de GBA. Het artikel schrijft niet voor dat de klacht een vermeende inbreuk op een wettelijke bepaling moet bevatten.

[2] Zie bijv Beheersplan 2021 van de GBA, p.18.

12. De Geschillenkamer zal derhalve bij beoordeling van de gegrondheid van de klacht, niet nagaan of de klagers in de formeel bij de GBA ingediende klacht wel de juiste wettelijke bepaling hebben ingeroepen als ondersteuning van hun verzoek, maar wel of de betrokken feiten een inbreuk vormen op een van de wettelijke bepalingen waarvan de GBA de naleving moet controleren. De Geschillenkamer wijst er daarbij nog op dat de controle op de naleving van de AVG de hoofdtaak is van dit orgaan van een toezichthouder.

13. In een eerdere beslissing overwoog de Geschillenkamer als volgt :

"Zo ook hoeven de klagers niet alle pertinente feiten van de beweerde inbreuk in hun klacht aan te voeren. De Geschillenkamer moet hen kunnen helpen door gerichte vragen te stellen om een goed begrip in feite en in rechte te krijgen van de mogelijke inbreuk op een grondrecht waarvoor haar aandacht wordt gevraagd. De Geschillenkamer kan ook rekening houden met grieven die later bij conclusie door de klager worden uiteengezet, op voorwaarde dat het gaat om feiten of juridische argumenten in verband met de beweerde inbreuk die is voorgelegd in de klacht, en met naleving van de rechten van de verdediging."

"Tijdens de op de klacht volgende procedure heeft de Geschillenkamer dus de mogelijkheid om de juridische kwalificatie van de haar voorgelegde feiten te veranderen, of nieuwe feiten in verband met de klacht te onderzoeken, zonder noodzakelijkerwijs een beroep te doen op de tussenkomst van de Inspectiedienst, meer bepaald door vragen te stellen aan de partijen of door rekening te houden met nieuwe feiten of kwalificaties die bij conclusie worden ingeroepen, en dit binnen de grenzen van het contradictoir debat, namelijk voor zover de partijen de gelegenheid hebben gekregen om te debatteren over deze feiten of juridische kwalificaties op een wijze die in overeenstemming is met de rechten van de verdediging. Indien nodig is het aan de Geschillenkamer om aan te zetten tot dit debat, hetzij in zijn brief met het verzoek conclusies in te dienen op basis van artikel 98 van de WOG, hetzij later in het kader van een heropening van de debatten. In deze context doet het feit dat rekening wordt gehouden met een nieuwe juridische kwalificatie, ingeroepen door de klager geen afbreuk aan het eerlijke verloop van de procedure en de gelijkheid van wapens, a fortiori aangezien de beslissingen van de Geschillenkamer ontvankelijk zijn voor een beroepsprocedure bij het Marktenhof[3]."

14. De Geschillenkamer oordeelt - anders dan verweerder - dat verweerder zich *in casu* volledig en tegen alle tenlastegelegde inbreuken heeft kunnen verweren en er geen sprake is geweest van achteraf bekend geworden nieuwe feiten waartegen verweerder zich niet heeft kunnen

[3] Beslissing 17/2020 van de Geschillenkamer
https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-17-2020.pdf

verdedigen. Verweerder heeft immers middels de door haar ingediende conclusie van antwoord op 27 mei 2020 uitvoerig alle (mogelijke) inbreuken besproken en verweer gevoerd tegen de klacht en de tenlastelegging. Verweerder heeft bij conclusie namelijk - kort samengevat - betoogd dat alle nodige technische en organisatorische maatregelen en overige voorzorgsmaatregelen door hen werden getroffen teneinde schending van de privacy te voorkomen. Volgens verweerder werd derhalve gehandeld conform de artikelen **5.1.f, 5.2, 24, 32, 33 en 34 AVG.** Bovendien heeft verweerder erkend dat er sprake is van een gegevenslek. Zij heeft echter betwist dat er sprake was van een gegevenslek die een waarschijnlijk hoog risico inhoudt in verband met de persoonsgegevens en waarvan melding bij de Gegevensbeschermingsautoriteit gedaan had moeten worden (artikel 33 AVG). Een andere reden om geen melding te doen was volgens verweerder dat de Gegevensbeschermingsautoriteit eerder in een vergelijkbaar geval van een gegevenslek waarbij wel melding werd gedaan, geen verdere maatregelen had genomen jegens verweerder.[4]

De inhoud van de zaak

15. 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.

16. 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 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 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, 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

[4] zie hierover verder randnummer [37].

simkaart van klager afgesloten. De klager had geen contact meer met het netwerk vanaf dat moment.

17. 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 eerst op 19 september dat klager opnieuw kon beschikken over zijn telefoonnummer.

18. Verweerder heeft op vraag van de Geschillenkamer tijdens de hoorzitting uitleg gegeven over de standaardprocedure die wordt gehanteerd in gevallen vergelijkbaar als deze. Verweerder stelt - zoals reeds eerder bij conclusie aangegeven - 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 gekregen. 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[5] en het Verslag aan de Koning bij het koninklijk besluit dat uitvoering aan deze wet geeft.[6]

19. 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.

---

[5] Artikel 127 juncto artikel 126 § 2,7° *Wet betreffende de elektronische communicatie* van 13 juni 2005, in werking getreden op 30 juni 2005.
[6] 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.

20. Tijdens de hoorzitting heeft verweerder te kennen gegeven dat het ingeven van het simkaartnummer door de medewerker van een Y shop een verplicht veld ("mandatory") is om een migratie van prepaid naar postpaid te doen. De medewerker dient derhalve de gegevens voor dit veld op te vragen bij de klant en effectief in te vullen om het contract voor het postpaid paid abonnement te kunnen afsluiten, aldus verweerder. De medewerker van een Y-shop kan volgens verweerder ook geen query's uitvoeren naar prepaid-databanken om het simkaartnummer op te vragen aan de hand van het gsm-nummer. De medewerker kon volgens verweerder het simkaartnummer – indien de derde dit niet zelf zou hebben opgegeven - enkel bekomen hebben door te bellen naar andere Y medewerkers om dit op te vragen. De kans dat een medewerker de derde zou hebben geholpen acht verweerder echter klein, met name omdat de medewerker daar geen commissie voor zou kunnen krijgen. Bovendien stelt de verweerder dat er in de dagen en uren rond de migratieaanvraag geen consultatie heeft plaatsgevonden van de gegevens van de klager.

21. Uitgaande van de verklaring van verweerder dat de winkelmedewerkers verplicht het simkaartnummer dienen op te vragen bij de klant en in te voeren om een migratie te bewerkstelligen van prepaid naar postpaid, en er geen mogelijkheid voor de medewerker is om aan de hand van het gsm-nummer het simkaartnummer op te vragen in de databank, blijft de vraag rijzen hoe de derde aan de combinatie gsm-nummer – simkaartnummer is gekomen.

22. Op de vraag van de Geschillenkamer tijdens de hoorzitting of er mogelijk sprake kan zijn geweest van een probleem van vertrouwelijkheid van gegevens op het niveau of in de systemen van Y – bijvoorbeeld via ongeoorloofde toegang tot het online klantenportaal waardoor het simkaartnummer kon worden bemachtigd - werd door verweerder ontkennend geantwoord. Op het klantenportaal van Y (zowel via de webbrowser als de mobiele applicatie) wordt volgens verweerder geen simkaartnummer vermeld. Bovendien geeft verweerder op de hoorzitting te kennen dat er geen meldingen zijn binnengekomen bij verweerder van andere klanten omtrent mogelijke gevallen van ongeoorloofde toegang tot hun simkaartnummer.

23. Een ander scenario is volgens verweerder dat de derde met kwade bedoelingen fraude heeft gepleegd door op één of andere (ongekende) manier aan de combinatie telefoon- en simkaartnummer van klager te komen. De Geschillenkamer stelt echter vast dat de derde wel zijn eigen naam, adres en woonplaats heeft opgegeven waardoor vanaf 11 september alle facturen bij hem terecht kwamen (en de klager tussen 11 en 15 september zelfs in principe op kosten van de derde kon gebruik maken van de diensten van Y). Dit maakt fraude in hoofde van de derde minder aannemelijk. Tijdens de hoorzitting brengt verweerder naar voren dat de derde weliswaar zijn eigen persoonsgegevens aan verweerder had doorgegeven, doch dat dit niet wegneemt dat nog altijd sprake kon zijn van een geval van fraude. De derde kreeg volgens verweerder namelijk

een mobiel telefoontoestel bij het afsluiten van het postpaid-abonnement. Het principe daarbij is dat na het betalen van twee jaren abonnementskosten het toestel ook zou zijn afbetaald. Volgens verweerder heeft de derde de facturen die in rekening werden gebracht voor het postpaid-abonnement nooit betaald. Verweerder geeft te kennen een procedure te zijn gestart tegen de derde voor het niet betalen van de facturen. De Geschillenkamer begrijpt in dit scenario echter niet waarom het nodig was dat de derde het telefoonnummer van klager moest overnemen. Het bekomen van het smartphonetoestel kon in dit geval ook eenvoudig door een postpaid-abonnement met een nieuw gsm-nummer aan te vragen.

24. De Geschillenkamer acht deze fraudehypothese met de bedoeling om een smartphone te bemachtigen door de overname van het gsm-nummer van klager *in casu* dus vrij onwaarschijnlijk, te meer nu de derde zijn eigen persoonsgegevens opgaf en een overeenkomst aanging voor het mobiele abonnement. Dit brengt met zich mee dat vanaf 11 september ook de kosten voor zijn rekening kwamen.

25. Verweerder heeft zowel bij conclusie als 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. Als oorzaak daarvan wijst verweerder de verboden die zijn opgelegd door artikel 127 van de Wet Elektronische Communicatie en het uitvoerend Koninklijk Besluit[7]. Het uitvoerend besluit bevat nadere regels omtrent de identificatie van de eindgebruikers van voorafbetaalde (prepaid) kaarten.[8] Volgens verweerder schrijven de wet en de besluiten voor dat identificatiegegevens niet mogen gebruikt worden voor commerciële doeleinden. Verweerder stelt namelijk dat : "*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*."

26. 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 …….". 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

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

[8] 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.

factuur wordt verstuurd) of de algemene wetgeving rond de bescherming van de persoonlijke levenssfeer."

27. Tijdens de hoorzitting heeft verweerder desgevraagd 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.

28. 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 niet juist.

29. De Geschillenkamer stelt zich de vraag of hier inderdaad sprake is van een commercieel doeleinde, gezien het gebruik van de identiteitsgegevens van een prepaid-klant *in casu* enkel het voorkomen van misbruik als doel zou hebben door iemand die zich in een Y shop mogelijks onterecht aanbiedt als zijnde de gebruiker van het telefoonnummer, gekoppeld aan een vooraf betaalde kaart. 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 (zie verder hieronder) met dus toegang tot zijn persoonsgegevens. 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 authenticatiemiddel is). Het gaat hier immers om een gerechtvaardigd doeleinde, namelijk het detecteren van mogelijke fraude met telefoonnummers welke enorme gevolgen voor betrokkenen kan hebben.

30. Hierbij wijst de Geschillenkamer tevens op het Verslag aan de Koning bij het uitvoerend Koninklijk Besluit.[9] 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 volgens de Geschillenkamer eveneens voorbij gegaan aan de wil van de wetgever, namelijk het bieden van een goed beschermingsniveau van persoonsgegevens aan betrokkenen. In een geval als dit strekt de –

[9] 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.

31. De Geschillenkamer is van mening dat verweerder *in casu* simpel had kunnen nagaan of de gegevens op de identiteitskaart van de derde (na verificatie van de foto op de identiteitskaart) overeen kwamen met de gekende gegevens van de houder van het telefoonnummer van de vooraf betaalde kaart. 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. 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. De Geschillenkamer acht deze nalatigheid disproportioneel.

32. Verweerder heeft bij conclusie van antwoord 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 confidentialiteit van de gegevens binnen de organisatie van verweerder te waarborgen.

33. 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".*

34. *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 volgens de Geschillenkamer verwijtbaar nalatig gehandeld.

35. 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 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.

36. 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 welke hij de communicatie via de applicatie wenst te gebruiken, 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.

37. 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, (bijvoorbeeld doordat er bijvoorbeeld potentieel gesprekken en berichten in naam van de benadeelde 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.

38. 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."*[10] 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 is van een significant gevaar voor de schending van zijn privacyrechten.

---

[10] 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.

39. 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."

40. 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.

41. 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.[11] 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 enkel één 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.[12] Bovendien betreft het hier volgens de Geschillenkamer 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 geraakt.

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

[12] Idem, p. 30

42. Verweerder legt een eerdere melding d.d. 11 maart 2019 aan de Gegevensbeschermingsautoriteit van een soortgelijk gegevenslek over.[13] 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.

43. 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 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.

44. 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*".[14]

---

[13] Als stuk 5 bij haar conclusies.

[14] 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.

45. De Geschillenkamer is van oordeel dat verweerder er in onderhavig geval niet in is geslaagd aan te tonen dat er proactieve maatregelen zijn 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 ingebracht waaruit blijkt dat is voldaan aan de documentatieplicht die op verweerder rustte. Het enige document dat door verweerder werd ingebracht 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 waarin is bepaald dat :

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

46. 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"[15] De Geschillenkamer is van oordeel dat zulks in onderhavig geval niet kan worden aangetoond.

47. 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.

---

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

48. 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.

49. De Geschillenkamer stelt derhalve inbreuken vast op artikel 33, leden 1 en 5, en 34, lid 1 en 2, 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 gevoeligheid hebben voor betrokkenen, onder meer omdat ze een regelmatige en stelselmatige observatie mogelijk maken.[16] Ook had de klager volgens artikel 34.1 op de hoogte gebracht moeten worden van het gegevenslek. Niettegenstaande het feit dat klager reeds op de hoogte was van het gegevenslek door te bellen met zijn eigen nummer, had verweerder de mededeling ervan alsnog en onverwijld, moeten doen conform de eisen van artikel 34 lid 2. Voornoemd artikel bepaalt namelijk dat de mededeling; de aard van de inbreuk; de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen en de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen dient te bevatten.

50. De Geschillenkamer leidt uit het niet inbrengen in de procedure van een mededeling in de zin van artikel 34 AVG door verweerder redelijkerwijs af dat zulks een mededeling niet aan klager is gedaan. Verweerder heeft derhalve nagelaten om nadat hij zelf op de hoogte raakte, klager middels een mededeling conform artikel 34 lid 2 op de hoogte te stellen van de toekenning van het telefoonnummer aan een derde. De Geschillenkamer verwerpt de stelling van verweerder dat een melding aan betrokkene in casu niet noodzakelijk was daar het niet zou gaan om een hoog risico. De Geschillenkamer verwijst in dit kader naar het volgende voorbeeld in de recentelijk gepubliceerde "*Guideline on Examples regarding Data Breach Notification"* van de EDPB waarin het contactcentrum van een telecommunicatie bedrijf wordt gebeld door een persoon die zegt een klant te zijn en vraagt een wijziging van zijn emailadres 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 emailadres

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

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.

51. 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."[17]

52. De melding van inbreuken moet worden gezien als een manier om de naleving van de regels inzake de bescherming van persoonsgegevens te verbeteren. 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, 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 stellen van de inbreuk. Daardoor kan de toezichthoudende autoriteit haar taken en bevoegdheden, zoals vastgelegd in de AVG, naar behoren uitvoeren.

4. Inbreuken op de AVG

[17] EDPB *Guideline on Examples regarding Data Breach Notification,* 01/2021, p.30
Onderlijning door de Geschillenkamer

53. 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 en 34.1 AVG**, ; gezien verweerder geen melding maakte van het gegevenslek aan de GBA en de betrokkene.

54. De Geschillenkamer acht het passend om een administratieve geldboete op te leggen ten bedrage van 25.000 Euro (artikel 83, lid 2 AVG; artikel 100, §1, 13° WOG en artikel 101 WOG).

55. Rekening houdend met artikel 83 AVG en de rechtspraak[18] van het Marktenhof, motiveert de Geschillenkamer het opleggen van een administratieve geldboete *in concreto*:

    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 zowel bij conclusie als tijdens de hoorzitting 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 en het bevel de verwerking in overeenstemming te brengen zijn volgens de Geschillenkamer dermate afschrikwekkend om dergelijke inbreuken in de toekomst te voorkomen.

56. 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.

57. 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

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

kernactiviteit uit van de verweerder waardoor het van doorslaggevend belang is dat de persoonsgegevens worden verwerkt conform de AVG.

58. 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 worden gesanctioneerd, opdat praktijken met dergelijke inbreuken niet zouden worden herhaald.

59. 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.

60. Verweerder heeft in haar reactie op de voorgenomen geldboete verzocht om de beslissing niet te publiceren, ook niet in geanonimiseerde vorm. De Geschillenkamer wijst dit verzoek af, met verwijzing naar de door haar op de website van de GBA gepubliceerde nota over publicatie van beslissingen, waarin is opgenomen dat : "*De Geschillenkamer gaat uit van het principe dat al haar beslissingen, op enkele uitzonderingen na, op haar website worden gepubliceerd, met het oog op het algemene doel inzake transparantie, maar ook zichtbaarheid en verantwoordingsplicht.*"[19]

OM DEZE REDENEN,

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

- Op grond van artikel 100, §1, 9° WOG, te bevelen de verwerking in overeenstemming te brengen met artikelen 5.1.f, 5.2, 24 en 32 AVG, waarbij in het bijzonder het beleid ten aanzien van de identificatie en verificatie van prepaid klanten in overeenstemming met de AVG wordt gebracht. Hiervoor geeft de Geschillenkamer de verweerder een termijn van drie

[19] https://www.gegevensbeschermingsautoriteit.be/publications/beleid-van-de-geschillenkamer-inzake-de-publicatie-van-de-beslissingen.pdf

maanden en verwacht de Geschillenkamer dat de verweerder haar rapporteert binnen dezelfde termijn omtrent het in overeenstemming brengen van de verwerking met voormelde bepalingen.

- op grond van artikel 83 AVG en artikelen 100, 13° en 101 WOG een administratieve geldboete **van 25.000 EUR** op te leggen aan de verweerders wegens de inbreuken op de artikelen 5.1.f, 5.2, 24, 32, 33.1 en 5, 34.1 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