Geschillenkamer

Beslissing ten gronde 18/2020 van 28 april 2020

Dossiernummer : AH-2019-0013

Betreft : Risicobeoordeling door Y betreffende melding van gegevenslekken

De Geschillenkamer van de Gegevensbeschermingsautoriteit, samengesteld uit de heer Hielke Hijmans, voorzitter en de heren Dirk Van Der Kelen en Jelle Stassijns, leden;

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

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit,* 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:

Y, hierna "de verweerder"

1. Feiten en procedure

A. Onderzoek van de Inspectiedienst

Op 11 juli 2019 besliste het Directiecomité van de Gegevensbeschermingsautoriteit (hierna GBA) om een zaak aanhangig te maken bij de Inspectiedienst van de GBA op basis van artikel 63, 1° WOG.

Na behandeling van het dossier door de Eerstelijnsdienst bleken er immers drie ernstige punten te zijn die een correcte naleving van de AVG in de weg staan:

1. de niet-naleving van de medewerkingsplicht (artikel 31 AVG);
2. de niet-naleving van zowel de verantwoordingsplicht (artikel 5.2 AVG) als de medewerkingsplicht (artikel 31 AVG) wat betreft het toepassing van de "risk based approach" bij de beveiliging van persoonsgegevens (artikel 36 AVG);
3. de niet-naleving van de verplichting van de verweerder om een belangenconflict in hoofde van de functionaris voor gegevensbescherming te vermijden (artikel 38.6 AVG) en het niet afdoende betrekken van de functionaris voor gegevensbescherming (artikel 38.1 AVG).

De aanleiding voor de voormelde aanhangigmaking was een concreet gegevenslek bij de verweerder. Dit lek werd ook wel het W incident genoemd. Dit gegevenslek vond plaats naar aanleiding van een aantal uitnodigingen die door de verweerder werden verstuurd naar o.a. zelfstandigen en vrije beroepers teneinde over te schakelen van een papieren naar een elektronische factuur. Door een fout in de selectie van de e-mailadressen werden een aantal van de uitnodigingen gelinkt aan vrije beroepers en zelfstandigen (en vervolgens ook de elektronische factuur) verstuurd naar secundaire e-mailadressen die in de databanken van de verweerder verbonden werden met een klant, maar mogelijks geen directe link hebben met de betrokken klant. Dergelijke secundaire contactpersonen zijn administratieve of technische contactpersonen voor de klant.

De communicatie die omtrent dit gegevenslek werd gevoerd tussen de Eerstelijnsdienst van de GBA en de verweerder gaf aanleiding tot een nota die door de Eerstelijnsdienst werd voorgelegd aan het Directiecomité met het voorstel om het bestaan van ernstige aanwijzingen te beoordelen en het dossier vervolgens voor te leggen aan de Inspectiedienst teneinde de aanpak van gegevenslekken door de verweerder te laten onderzoeken (artikel 63, 1° WOG).

De Inspectiedienst maakte haar verslag d.d. 6 september 2019 aan de Geschillenkamer over op basis van artikel 91, §2 WOG, waardoor de Geschillenkamer werd gevat op grond van artikel 92, 3° WOG.

B. Procedure voor de Geschillenkamer

Ter zitting van 24 september 2019 besliste de Geschillenkamer op grond van artikel 95, §1, 1° WOG en artikel 98 WOG dat het dossier gereed was voor behandeling ten gronde.

Op dezelfde dag werd de verweerder per aangetekende zending in kennis gesteld van deze beslissing, alsook van het inspectieverslag en van de inventaris van de stukken van het dossier dat door de Inspectiedienst aan de Geschillenkamer werd overgemaakt. Tevens werd de verweerder in kennis gesteld van de bepalingen zoals vermeld in artikel 98 van de WOG en werd verweerder op grond van artikel 99 van de WOG in kennis gesteld van de termijnen om zijn verweermiddelen in te dienen. De uiterste datum voor ontvangst van de conclusie van antwoord van de verweerder werd op 28 oktober 2019 vastgesteld.

Op 29 oktober 2019 ontving de Geschillenkamer de conclusie van antwoord van de verweerder. Deze conclusie bevat naast het inhoudelijke verweer omtrent de drie vaststellingen van de Inspectiedienst aangaande de medewerkingsplicht (1), de verantwoordingsplicht en de verantwoordelijkheid van de verwerkingsverantwoordelijke (2) en de positie van de functionaris voor gegevensbescherming (3), ook een procedureel verweermiddel waarin de verweerder opwerpt dat in dit dossier de door de wetgever afgebakende bevoegdheidsverdeling tussen de Eerstelijnsdienst en de Inspectiedienst niet werd gerespecteerd, hetwelk zou leiden tot de onbevoegdheid van de Geschillenkamer en tot ontoelaatbaarheid van het verslag van de Inspectiedienst en van de interne nota van de Eerstelijnsdienst.

Op 14 februari 2020 wordt het dossier hernomen en vindt de hoorzitting plaats. De verweerder wordt aldus gehoord en krijgt de gelegenheid om zijn argumenten naar voor te brengen.

Vervolgens wordt de zaak door de Geschillenkamer in beraad genomen.

Op 18 februari 2020 wordt ingevolge artikel 54 van het reglement van interne orde van de Gegevensbeschermingsautoriteit aan de verweerder een kopie van het proces-verbaal van de hoorzitting overgemaakt.
De verweerder krijgt hierbij de gelegenheid om zijn eventuele opmerkingen daaromtrent te laten toevoegen als bijlage bij het proces-verbaal, zonder dat dit een heropening van de debatten inhoudt.

Op 21 februari 2020 ontvangt de Geschillenkamer vanwege de verweerder enkele opmerkingen met betrekking tot het proces-verbaal, dewelke zij beslist mee op te nemen in haar beraad en haar beslissing.

Op 26 februari 2020 bezorgt de verweerder, zoals gevraagd tijdens de hoorzitting, het correcte ondernemingsnummer en de jaaromzet van de drie laatste boekjaren. Deze bedragen:

voor 2017: € 4.058.643.958
voor 2018: € 4.009.935.363
voor 2019: € 3.886.699.793

Op 3 april 2020 heeft de Geschillenkamer aan de verweerder het voornemen kenbaar gemaakt om over te gaan tot het opleggen van een administratieve geldboete, alsmede het bedrag daarvan teneinde de verweerder de gelegenheid te geven zich te verdedigen, voordat de sanctie effectief wordt opgelegd en uitgevoerd.

Op 24 april 2020 ontving de Geschillenkamer de reactie van de verweerder op het voornemen tot het opleggen van een administratieve geldboete, alsmede het bedrag daarvan. De verweerder stelt het oneens te zijn met het opleggen van een geldboete, of de voorgenomen hoogte van de geldboete, en hij verwijst hiervoor naar zijn conclusies. Hij voert echter geen (nieuwe) argumenten aan ter onderbouwing van deze stelling. De reactie van de verweerder geeft voor de Geschillenkamer dan ook geen aanleiding tot aanpassing van het voornemen tot het opleggen van een administratieve geldboete en evenmin tot wijziging van het bedrag van de boete zoals voorgenomen.

2. Rechtsgrond

Artikel 38.6 AVG

6. De functionaris voor gegevensbescherming kan andere taken en plichten vervullen. De verwerkingsverantwoordelijke of de verwerker zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden.

3. Motivering

a) Procedure

Als eerste verweermiddel voert de verweerder aan dat de procedure een aantal gebreken zou vertonen. De verweerder werpt op dat de Eerstelijnsdienst verder is gegaan dan de loutere

behandeling van het meldingsdossier, zodanig dat van het W Incident niets meer terug te vinden is in de bezwaren die aan de basis liggen van de procedure voor de Geschillenkamer. Uit de schriftelijke bevraging, meer bepaald de omvang van de bevraging en het aantal aanvullende vragen gesteld aan de verweerder, blijkt volgens de verweerder dat de Eerstelijnsdienst onderzoek heeft gevoerd, hetgeen conform artikel 66, §1, 3° WOG een onderzoeksbevoegdheid is van de Inspectiedienst.

Alsook zou de Eerstelijnsdienst gebruik hebben gemaakt van de onderzoeksmodaliteit tot het identificeren van personen, hetwelk een bevoegdheid is die toekomt aan de Inspectiedienst (artikel 66, §1, 1° WOG). De verweerder stelt dat zijn argumentatie – namelijk dat het onderzoek al werd gevoerd op het niveau van de Eerstelijnsdienst en dus vooraleer het dossier bij de Inspectiedienst terecht kwam – wordt bevestigd doordat het verslag van de Inspectiedienst voor de *"onderzoeksmaatregelen i.f.v. het onderzoek"* uitsluitend naar het *"doornemen van het dossier ontvangen via het directiecomité"* verwijst. Volgens de verweerder baseert de Inspectiedienst zijn verslag dus louter en alleen op een onderzoek dat werd gevoerd door de Eerstelijnsdienst.

De verweerder voegt tijdens de hoorzitting daaraan toe dat de interne nota vanuit de Eerstelijnsdienst, dewelke is gericht aan het Directiecomité en dus op het ogenblik dat het dossier nog niet aanhangig was gemaakt bij de Inspectiedienst, werd verzonden met reeds de vermelding van de contactgegevens van de Inspectiedienst (inspection@apd-gba.be). Het uitvoeren van onderzoeksdaden door een dienst die deze wettelijk gezien niet mag uitvoeren wordt door de verweerder bestempeld als fishing expedition.

De Eerstelijnsdienst heeft volgens de verweerder dan ook haar bevoegdheid overschreden en zich niet gehouden aan haar wettelijke bevoegdheden, meer bepaald haar bevoegdheid tot het opstarten van een bemiddelingsprocedure (artikel 22, 2° WOG). De verweerder haalt aan dat op herhaalde verzoeken tot overleg vanwege hemzelf niet werd ingegaan door de Eerstelijnsdienst.

Bovendien heeft ook de Inspectiedienst volgens de verweerder zijn bevoegdheden niet gerespecteerd doordat de Inspectiedienst zich uitsluitend op het dossier van de Eerstelijnsdienst heeft gebaseerd voor het opstellen van het verslag. Dit brengt de verweerder ertoe om te stellen dat de Inspectiedienst geen onderzoek heeft gevoerd, omdat geen van de onderzoeksmaatregelen in artikel 66, § 1 WOG werden genomen. De verweerder argumenteert dat de Inspectiedienst aldus niet bevoegd was om zijn verslag op te stellen, daar het zijn onderzoek niet rechtmatig had kunnen afronden, omwille van een gebrek aan enige onderzoeksmaatregel.

De verweerder stelt dat de Geschillenkamer niet rechtsgeldig werd gevat en zich onbevoegd dient te verklaren omdat:

- De Inspectiedienst geen onderzoek voerde;

- De Inspectiedienst niet bevoegd was om zijn onderzoek af te sluiten;
- De Geschillenkamer slechts na een rechtmatige afsluiting van het onderzoek gevat kon worden.

De verweerder werpt subsidiair op dat het verslag van de Inspectiedienst en de interne nota van de Eerstelijnsdienst ontoelaatbaar zijn wegens schending van de fundamentele rechtsprincipes, in het bijzonder van het principe van eerlijke rechtsbedeling en het recht van verdediging, alsook van de algemene beginselen van behoorlijk bestuur, waarbij de Geschillenkamer als administratieve overheid in het bijzonder het zorgvuldigheids- en onpartijdigheidsbeginsel dient te respecteren.

Er wordt tijdens de hoorzitting door de verweerder niet ontkend dat er onderzoek is gedaan, maar hij stelt dat het op de verkeerde wijze is gebeurd. De verweerder voert aan dat de Geschillenkamer niet bevoegd is wanneer de verzamelde elementen zijn verkregen op wettelijk onjuiste wijze. De documenten van de Eerstelijnsdienst moeten dan ook volgens de verweerder uit het onderzoek worden geweerd en hij benadrukt dat de Eerstelijnsdienst moet optreden binnen haar bevoegdheden zoals vastgelegd in artikel 22 WOG. De naleving hiervan is voor de verweerder essentieel met het oog op rechtszekerheid. De verweerder stelt uitdrukkelijk dat het belangrijk is voor een onderneming om in dialoog te kunnen treden met een departement binnen de GBA zonder dat er meteen een onderzoek wordt gevoerd, zodanig dat er mogelijkheid is tot samenwerking, overleg en bemiddeling.

De Geschillenkamer benadrukt dat een onpartijdige en eerlijke behandeling over het volledige traject moet worden verzekerd. Het door de verweerder opgeworpen probleem heeft betrekking op de voorafgaande fase, maar de rechten van verdediging zijn niet geschonden, want de verweerder heeft de kans gekregen om zijn argumentatie volledig naar voor te brengen door middel van zijn conclusie van antwoord en daarenboven heeft hij zijn recht op tegenspraak ten volle kunnen uitoefenen tijdens de hoorzitting van de Geschillenkamer.

De Geschillenkamer kan enkel vaststellen dat in het geval waarin de GBA ambtshalve kan optreden, de wettelijk voorziene procedure is gerespecteerd, namelijk dat wanneer het Directiecomité ernstige aanwijzingen vaststelt van het bestaan van een praktijk die aanleiding kan geven tot een inbreuk op de grondbeginselen van de bescherming van de persoonsgegevens, in het kader van de WOG en van de wetten die bepalingen bevatten inzake de bescherming van de verwerking van persoonsgegevens, de aanhangigmaking bij de Inspectiedienst kan gebeuren (artikel 63, 1° WOG). In toepassing daarvan werd door de beslissing van het Directiecomité genomen op 11 juli 2019, het dossier aanhangig gemaakt bij de Inspectiedienst op 12 augustus 2019, zonder dat daarbij een procedureregel werd geschonden die van aard zou zijn de belangen van de verweerder te schaden of zijn rechten te schenden. De fundamentele procedurele waarborg bestaande uit het verzekeren van het recht van tegenspraak is daarbij nageleefd doordat het inspectieverslag door de Geschillenkamer aan de

verweerder werd overgemaakt en hij de gelegenheid heeft gehad om te reageren op elk van de daarin opgenomen vaststellingen van de Inspectiedienst.

De Geschillenkamer is dan ook van oordeel dat de voorliggende kennisgeving van een mogelijke inbreuk in verband met persoonsgegevens is behandeld met naleving van alle fundamentele rechtsprincipes en algemene beginselen van behoorlijk bestuur.

b) Medewerking met de toezichthoudende autoriteit (artikel 31 AVG)

De Inspectiedienst doet omtrent de medewerkingsplicht de volgende vaststelling in haar verslag:

"De verweerder heeft verschillende middelen gebruikt om de verplichte medewerking met de GBA te bemoeilijken. Die middelen worden op de webpagina's http://www.aalep.eu/recognizing-your-opposition-tactics-and-responding-them en https://ctb.ku.edu/en/table-of-contents/advocacy/respond-to- counterattacks/ overview-of-opposition-tactics/main beschreven als de "Ten D's".

Bij een beoordeling van de contacten met de verweerder kan worden vastgesteld dat de verweerder 5 van de 10 technieken toepaste.

Het komt volgens de Inspectiedienst toe aan de Geschillenkamer om uit te maken of de toepassing van de voormelde technieken een inbreuk inhoudt op de medewerkingsplicht, dan wel kan worden beschouwd als een normale uitoefening van het recht van verdediging van de verweerder op basis van de toepasselijke algemene rechtsbeginselen."

De verweerder voert omtrent deze vaststellingen van de Inspectiedienst inzake medewerking vooreerst aan dat gelet op het feit dat de Eerstelijnsdienst haar bevoegdheid te buiten ging en dus niet de haar toegewezen taken vervulde, hij niet diende mee te werken en niet diende in te gaan op de vragen van de Eerstelijnsdienst. Ten tweede betwist de verweerder de juridische waarde van de webpagina's waarop de GBA zich baseert en argumenteert hij dat hij wel zijn medewerking heeft verleend en geen van de vijf door de Inspectiedienst vermelde "Ten D's" technieken heeft toegepast. De verweerder stelt dat de vereiste van medewerking in ieder geval wordt begrensd door het recht van verdediging en het recht op niet-zelfincriminatie, dat van toepassing is in administratieve procedures die aanleiding kunnen geven tot het opleggen van administratieve geldboetes. Door de verregaande vraagstellingen zou het recht van verdediging en het verbod op zelf-incriminatie zijn geschonden.

De Geschillenkamer heeft de vaststellingen van de Inspectiedienst in het licht van de

medewerkingsplicht van de verweerder beoordeeld en stelt vast dat de Inspectiedienst onvoldoende heeft aangetoond dat de verweerder door middel van antwoordbrieven niet heeft getracht om uitgebreid en omstandig te antwoorden op de gestelde vragen. Daarenboven verklaarde de verweerder zich meermaals bereid om in aanvulling daarop in overleg te treden, waardoor niet kan worden vastgesteld dat hij niet is tegemoet gekomen aan de verplichting tot medewerking met de toezichthoudende autoriteit.

De Geschillenkamer oordeelt dan ook dat er **geen inbreuk op artikel 31 AVG** kan worden vastgesteld. Dit oordeel is gebaseerd op feitelijke vaststellingen, waardoor het niet nodig is in deze zaak een principieel oordeel te geven over de omvang van de medewerkingsplicht.

c) Verantwoordingsplicht (artikel 5.2 AVG en artikel 24, lid 1 AVG) voor wat betreft de toepassing van de risico-inschatting bij de melding van een inbreuk in verband met persoonsgegevens (artikel 33 AVG)

Het inspectieverslag maakt omtrent deze ernstige aanwijzing vanwege het Directiecomité melding van de volgende vaststelling:

"De risico-inschatting door de verweerder bij de melding van inbreuken in verband met persoonsgegevens was het afgelopen jaar systematisch "laag" of "verwaarloosbaar laag". Hoe het team van de verweerder (bestaande uit vertegenwoordigers van de business) tot dit resultaat komt is, ondanks de vragen die daarover werden gesteld door de GBA, in concreto niet duidelijk. Zoals blijkt uit het schrijven van de verweerder van 12/06/2019 is hij niet bereid om dat verder toe te lichten omdat hij daartoe niet verplicht zou zijn onder de AVG. Uit de "RACI matrix" vermeld in voormeld schrijven blijkt bovendien dat de functionaris voor gegevensbescherming van de verweerder niet deelneemt aan de discussies rond de risico-inschatting ter zake aangezien hij enkel "informed" is in plaats van "consulted". Wie wat beslist bij de verweerder in een concreet dossier wordt niet meegedeeld aan de GBA en er is geen indicatie dat de verweerder die praktijk wenst te wijzigen.
Het wordt door het gebruik van vage omschrijvingen van het beoordelingsproces en ontkenningen voor de GBA onmogelijk gemaakt om na te gaan hoe de verweerder in een concreet dossier tot een bepaalde conclusie over het risico is gekomen.
De voormelde handelswijze is strijdig met de verantwoordingsplicht (artikel 5, lid 2 AVG) en de verantwoordelijkheid (artikel 24, lid 1 AVG) van de verweerder voor wat betreft de toepassing van de risico-gebaseerde benadering bij de beveiliging van persoonsgegevens (artikel 32 AVG)."

De verweerder merkt op dat het inspectieverslag enkel uitdrukkelijk verwijst naar de risico-gebaseerde benadering bij de *beveiliging* van persoonsgegevens (artikel 32 AVG), terwijl uit de inhoud van het

verslag blijkt dat het de risico-inschatting bij de *melding van inbreuken* in verband met persoonsgegevens betreft, hetgeen artikel 33 en 34 AVG betreft. Hierdoor zou het aan de verweerder onmogelijk worden gemaakt om zich goed te verdedigen met gevolgen voor de beslissing van de Geschillenkamer vanuit het perspectief van fundamentele rechtsbeginselen en de algemene beginselen van behoorlijk bestuur.

De Geschillenkamer oordeelt omtrent dit punt dat de conclusie van de verweerder, afgezien van deze vaststelling van de verweerder omtrent de toepasselijke wetsartikelen, geen enkel element bevat waaruit blijkt dat hij ook maar enig verweer voert omtrent de risico-gebaseerde benadering bij de *beveiliging* van persoonsgegevens (artikel 32 AVG). Het volledige verweer heeft betrekking op de risico-inschatting bij de *melding van inbreuken* in verband met persoonsgegevens (artikel 33 en 34 AVG). Uit geen enkel element blijkt dat er in hoofde van de verweerder enige twijfel bestond over de artikelen die aan de basis lagen van de vaststelling van de Inspectiedienst, zodanig dat op basis daarvan moet worden besloten dat de fundamentele rechtsbeginselen en de algemene beginselen van behoorlijk bestuur werden nageleefd. Dit wordt verklaard doordat alle stukken van het dossier betrekking hebben op de risico-inschatting bij de melding van inbreuken in verband met persoonsgegevens. Ook het inspectieverslag vermeldt bij aanvang van de vaststelling dat het de risico-inschatting bij de melding van inbreuken in verband met persoonsgegevens betreft en uit de context van het verslag blijkt duidelijk dat het enkel daarover gaat.

De verweerder stelt op inhoudelijk vlak dat er geen wettelijke verplichting is om een gedetailleerde verificatiemogelijkheid aan de GBA voor te leggen. Wel werd informatie over de methodologie voor de risico-analyse en de procedure betreffende deze analyse en de besluitvorming bezorgd aan de GBA. Niettegenstaande de betwisting van de bevoegdheid van de GBA, benadrukt de verweerder dat toch informatie werd bezorgd, waarbij hij aangaf in dialoog te willen treden omtrent de inschatting van de risico's. De verweerder gaat ook in op de stelling van de Inspectiedienst dat door het gebruik van vage omschrijvingen van het beoordelingsproces en ontkenningen de verweerder het voor de GBA onmogelijk wordt gemaakt om na te gaan hoe de verweerder in een concreet dossier tot een bepaalde conclusie is gekomen.

De verweerder verwijst in zijn conclusie naar de relevante stukken die deze stelling van de Inspectiedienst zouden ontkrachten en waardoor de GBA wel in de mogelijkheid was om na te gaan hoe de verweerder in een concreet dossier tot een bepaalde conclusie over het risico was gekomen. De verweerder concludeert dat er geen schending van de verantwoordingsplicht is, vermits artikel 5.2 AVG enkel betrekking zou hebben op de beginselen vermeld in artikel 5.1 AVG en niet op de regels betreffende de gevolgen van een inbreuk op persoonsgegevens.

De Geschillenkamer beklemtoont dat, in tegenstelling tot wat de verweerder stelt, er in hoofde van de verwerkingsverantwoordelijke wel degelijk een verplichting is om elk gegevenslek, ongeacht of dit risicovol is of niet, te documenteren teneinde informatie te kunnen verstrekken aan de GBA. Bovendien is artikel 5.2 AVG, eveneens in tegenstelling tot wat de verweerder stelt, niet beperkt tot de beginselen opgesomd in artikel 5.1 AVG, maar heeft artikel 5.2 AVG wel degelijk ook betrekking op de andere bepalingen van de AVG, waaronder artikel 33 AVG. Dit vloeit voort uit de nauwe samenhang tussen enerzijds artikel 5.2 AVG en anderzijds de verplichtingen voor de verwerkingsverantwoordelijke die voortvloeien uit de artikelen 24 en volgende van de AVG.

De Geschillenkamer verwijst hiervoor naar de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 van de Groep Gegevensbescherming Artikel 29[1] waarin het volgende wordt gesteld:

"Ongeacht of een inbreuk aan de toezichthoudende autoriteit moet worden gemeld, moet de verwerkingsverantwoordelijke alle inbreuken documenteren, zoals in artikel 33, lid 5, wordt uitgelegd:
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.
Dit hangt samen met het in artikel 5, lid 2, vervatte verantwoordingsbeginsel van de AVG. Het doel van de registratie van zowel niet te melden als te melden inbreuken houdt ook verband met de verplichtingen van de verwerkingsverantwoordelijke op grond van artikel 24. De toezichthoudende autoriteit kan verzoeken om inzage in deze geregistreerde gegevens. Verwerkingsverantwoordelijken worden er daarom toe aangemoedigd een intern register van inbreuken op te zetten, ongeacht of voor die inbreuken een meldingsplicht geldt.
Hoewel het aan de verwerkingsverantwoordelijke is om te bepalen welke methode en structuur bij het documenteren van een inbreuk moeten worden gebruikt, zijn er wat te registreren informatie betreft belangrijke elementen die in alle gevallen moeten worden opgenomen. Zoals vereist op grond van artikel 33, lid 5, dient de verwerkingsverantwoordelijke bijzonderheden met betrekking tot de inbreuk te registreren, waaronder de oorzaken, wat er zich heeft afgespeeld en de betrokken persoonsgegevens. De verwerkingsverantwoordelijke dient ook de gevolgen van de inbreuk te registreren, alsmede de corrigerende maatregelen die hij heeft genomen.
In de AVG is niet gespecificeerd hoelang deze documentatie moet worden bewaard. Indien deze geregistreerde gegevens persoonsgegevens bevatten, is het aan de

[1] WP250.Rev01, pp 30-32.

verwerkingsverantwoordelijke om de passende bewaartermijn te bepalen in overeenstemming met de beginselen voor de verwerking van persoonsgegevens en om te voldoen aan de rechtsgrond voor de verwerking. Hij dient de documentatie overeenkomstig artikel 33, lid 5, te bewaren voor zover de toezichthoudende autoriteit de verwerkingsverantwoordelijke kan verzoeken om het bewijs te leveren dat hij dat artikel, of meer in het algemeen het verantwoordingsbeginsel, naleeft. Als de geregistreerde gegevens geen persoonsgegevens bevatten, is het in de AVG opgenomen beginsel van opslagbeperking uiteraard niet van toepassing.

Naast deze details beveelt de WP29 aan dat de verwerkingsverantwoordelijke ook zijn motivering voor de besluiten die naar aanleiding van een inbreuk zijn genomen, documenteert. Met name wanneer inbreuk niet is gemeld, moet de motivering voor dat besluit worden gedocumenteerd. De motivering dient de redenen te omvatten waarom de verwerkingsverantwoordelijke van mening is dat de inbreuk waarschijnlijk geen risico voor de rechten en vrijheden van natuurlijke personen inhoudt. Indien de verwerkingsverantwoordelijke van mening is dat aan een van de voorwaarden van artikel 34, lid 3, is voldaan, moet hij afdoend bewijs kunnen leveren dat dit het geval is.

Als de verwerkingsverantwoordelijke een inbreuk niet meldt aan de toezichthoudende autoriteit maar de melding uitstelt, moet hij dat uitstel kunnen motiveren; documentatie in verband daarmee zou kunnen helpen om aan te tonen dat het uitstel gerechtvaardigd en niet buitensporig is.

Indien de verwerkingsverantwoordelijke een inbreuk aan de getroffen personen meedeelt, dient hij transparant te zijn over de inbreuk en doeltreffend en tijdig te communiceren. Bijgevolg zou het de verwerkingsverantwoordelijke helpen om aan te tonen dat hij het verantwoordingsbeginsel naleeft en zich aan de regels houdt door het bewijs van die mededeling te bewaren.

Ter ondersteuning van de naleving van de artikelen 33 en 34 zou het voor zowel verwerkingsverantwoordelijken als verwerkers nuttig zijn over een gedocumenteerde meldingsprocedure te beschikken waarin wordt uiteengezet welke procedure moet worden gevolgd wanneer een inbreuk is geconstateerd, met inbegrip van de wijze waarop het incident moet worden ingeperkt, beheerd en hersteld, het risico moet worden beoordeeld en de inbreuk moet worden gemeld. Om aan te tonen dat de AVG wordt nageleefd, kan het in dit verband ook nuttig zijn om aan te tonen dat werknemers op de hoogte zijn gebracht van het bestaan van dergelijke procedures en mechanismen en dat zij weten hoe zij op inbreuken moeten reageren.

Merk op dat het niet naar behoren documenteren van een inbreuk ertoe kan leiden dat de toezichthoudende autoriteit haar bevoegdheden op grond van artikel 58 uitoefent en/of een administratieve boete oplegt in overeenstemming met artikel 83." [onderstrepingen door Geschillenkamer].

In het licht van de voormelde richtsnoeren heeft de Geschillenkamer tijdens de hoorzitting aan de verweerder de vraag voorgelegd in welke mate gegevenslekken door hem worden gedocumenteerd.
De verweerder gaf aan dat alle bekende lekken worden gedocumenteerd en daartoe beroep wordt gedaan op de loyauteit en professionaliteit van de individuele werknemer om een mogelijk gegevenslek via de beschikbare tool binnen de onderneming te escaleren. De verweerder stelt over de nodige policies te beschikken en trainingen te organiseren om haar werknemers op te leiden omtrent het aangeven van datagerelateerde incidenten.

Gelet op deze toelichting verstrekt tijdens de hoorzitting, alsmede door het feit dat uit de stukken van het dossier blijkt dat de verweerder, ondanks zijn betwisting van de bevoegdheid van de GBA om gedetailleerde informatie op te vragen, is ingegaan op het verzoek om het beoordelingsproces te verduidelijken teneinde de GBA toe te laten om na te gaan hoe de verweerder in een concreet dossier, met name het W Incident, tot een bepaalde conclusie over het risico is gekomen, dient de Geschillenkamer te besluiten dat de verweerder zijn methodologie en procedure inzake inbreuken en de inschatting van risico's heeft uiteengezet.
De Geschillenkamer is bijgevolg van oordeel dat er **geen inbreuk op artikel 5.2 AVG, artikel 24.1 AVG en artikel 33 AVG** kan worden vastgesteld.

d) Positie van de functionaris voor gegevensbescherming (artikel 38 AVG)

Het verslag van de Inspectiedienst doet omtrent de positie van de functionaris voor gegevensbescherming de volgende vaststellingen:

De functionaris voor gegevensbescherming van de verweerder vervult naast die functie ook de functie van directeur audit, risk en compliance bij de verweerder.

Uit dit dossier blijkt dat de functionaris voor gegevensbescherming zich niet in een positie bevindt die voldoende vrij is van een belangenconflict (zoals opgelegd door artikel 38, lid 6 AVG) en onvoldoende wordt betrokken bij de discussies over inbreuken in verband met persoonsgegevens (zoals opgelegd door artikel 38, lid 1 AVG).

Onvoldoende betrokkenheid van de functionaris voor gegevensbescherming:

- *De functionaris voor gegevensbescherming van de verweerder wordt enkel geïnformeerd over het resultaat van de risicobeoordeling. We verwijzen in dat verband naar het schrijven van 12/06/2019 waarin het RACI matrix onder punt 1.4.2.2 aangeeft dat haar functionaris voor gegevensbescherming enkel "informed" is en niet "consulted". Artikel 38, lid 1 AVG vereist echter dat de DPO naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.*
- *De velden "advies van de DPO" werden tot voor kort systematisch niet ingevuld door de*

verweerder. Uit de toelichting onder punt 1.4.2.2 van het schrijven van de verweerder van 12/06/2019 (stuk 13) blijkt dat de discussie over het risico toebehoort aan de "business" (wat ook blijkt uit het voormelde RACI matrix) en dat het advies van haar functionaris voor gegevensbescherming tot voor kort niet was opgenomen in het modelformulier van de verweerder ("Personal Data Breach Investigation Report").

Belangenconflict bij de functionaris voor gegevensbescherming

- *<u>Conflicterende taken.</u> De verweerder stelt in zijn schrijven van 03/04/2019 en van 12/06/2019 dat zijn functionaris voor gegevensbescherming enkel een adviserende rol heeft en geen beslissingen kan nemen over het doel en de middelen van de verwerking wat ook vermeld wordt in de [Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO) van de Groep].[2] Het bestaan van een belangenconflict is echter niet beperkt tot de gevallen waar een persoon het doel en de middelen van de verwerking bepaalt. Belangenconflicten moeten steeds geval per geval worden beoordeeld. Het voormelde schrijven van de verweerder toont aan dat haar functionaris voor gegevensbescherming meer doet dan de verweerder intern te adviseren aangezien die persoon binnen Y (de verweerder) conflicterende taken uitvoert die een aanzienlijke operationele verantwoordelijkheid inhouden voor gegevensverwerkingsprocessen die vallen onder het domein audit, risk en compliance.*

  - *<u>Pragmatische benadering in Duitsland en in rechtsleer,</u>[3] die […] verwijzen naar criteria zoals (1) het al dan niet bestaan van zelfcontrole door een toonaangevende functiehouder binnen de onderneming, (2) het al dan niet bestaan van interne regels voor belangenconflicten, en (3) het dragen van een belangrijke operationele verantwoordelijkheid met een impact op persoonsgegevens, ...*

  - *<u>De verweerder had tot voor kort geen beleid om belangenconflicten te voorkomen.</u> Pas na aangetekende brieven van de GBA van 04/03/2019 en 16/05/2019 die de positie van de functionaris voor gegevensbescherming in vraag stelden werd via het schrijven van de verweerder van 12/06/2019 een <u>niet gedateerd</u> document "Y (verweerder) DPO Charter" bezorgd, dat nog moest worden geagendeerd voor het Audit en Compliance Comité in juli 2019 (zoals vermeld op pagina 6 van voormeld schrijven van de verweerder). Het opmaken van een dergelijk document impliceert niet dat daarmee afdoende is aangetoond dat de functionaris voor gegevensbescherming onafhankelijk werkt.*

---

[2] WP 243Rev01, pp 20-21.

[3] Persbericht van de Beierse toezichthoudende autoriteit van 20/10/2016 over een IT-manager gepubliceerd op https://www.lda.bayern.de/media/pm2016 OS.pdf en becommentarieerd op https://iapp.org/news/a/german-company-fined-for-dpo-conflict-of-interest/ alsook rechtsleer terzake (met name F. SCHRAM, De functionaris voor gegevensbescherming, Cahier editie 2, Politeia, 2019, 119-121).

In het verweer wordt aangaande de **betrokkenheid van de functionaris voor gegevensbescherming** beklemtoond dat de vaststelling van de Inspectiedienst is gebaseerd op een wettelijke en een feitelijke misinterpretatie.

Volgens de verweerder zou het, zoals uiteengezet in zijn conclusie, voor de toepassing van artikel 38.1 AVG volstaan dat de functionaris voor gegevensbescherming wordt geïnformeerd, als zijnde een onderdeel van betrokkenheid, maar legt deze bepaling niet de specifieke verplichting op om te worden geraadpleegd, in tegenstelling tot wat het inspectieverslag vermeldt.

De Geschillenkamer is van oordeel dat het standpunt van de verweerder niet in overeenstemming is met de *ratio legis* en geen zinvolle interpretatie is van artikel 38.1 AVG, dat bepaalt dat de functionaris "naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens". Door de betrokkenheid van de functionaris voor gegevensbescherming te herleiden tot het hem louter (achteraf) informeren over een beslissing, wordt zijn functie uitgehold.

De Geschillenkamer wijst daarbij in het bijzonder op de Richtlijnen van de Groep 29 voor functionarissen voor gegevensbescherming[4], die onderstrepen dat het van cruciaal belang is dat de functionaris voor gegevensbescherming zo vroeg mogelijk betrokken wordt bij alle aangelegenheden die met gegevensbescherming verband houden. Door ervoor te zorgen dat de functionaris voor gegevensbescherming van bij de start geïnformeerd en, nog belangrijker, geconsulteerd wordt, wordt de naleving van de algemene verordening gegevensbescherming mogelijk gemaakt.

Dit bevordert bovendien de naleving van een aanpak van gegevensbescherming door ontwerp, zoals voorzien in art. 25 AVG en die dan ook de standaardprocedure binnen het bestuur van de organisatie moet worden.

De Geschillenkamer stelt vast dat de verweerder artikel 38.1 AVG op onjuiste wijze heeft geïnterpreteerd. Echter, er is aan de Geschillenkamer in voldoende mate aannemelijk gemaakt dat, voor wat betreft het *risicobeoordelingsproces,* in de praktijk de functionaris voor

[4] "Het is van cruciaal belang dat de functionaris voor gegevensbescherming, of diens team, zo vroeg mogelijk betrokken wordt bij alle aangelegenheden die met gegevensbescherming verband houden. Wat betreft gegevensbeschermingseffectbeoordelingen, wordt in de algemene verordening gegevensbescherming expliciet vermeld dat de functionaris voor gegevensbescherming daarbij vroeg moet worden betrokken en gespecificeerd dat de verwerkingsverantwoordelijke bij de uitvoering van dergelijke effectbeoordelingen aan de functionaris voor gegevensbescherming advies moet vragen. Door ervoor te zorgen dat de functionaris voor gegevensbescherming van bij de start geïnformeerd en geconsulteerd wordt, wordt de naleving van de algemene verordening gegevensbescherming mogelijk gemaakt en wordt een privacy-aanpak door ontwerp bevorderd, die dan ook de standaardprocedure binnen het bestuur van de organisatie moet worden. Verder is het ook belangrijk dat de functionaris voor gegevensbescherming als een gesprekspartner binnen de organisatie wordt gezien en dat hij/zij deel uitmaakt van de relevante werkgroepen die zich met gegevensverwerking binnen de organisatie bezighouden.", WP24301 Rev, para 3.1. van de richtlijnen, onderstreping door Geschillenkamer.

gegevensbescherming wordt betrokken en zelf een onafhankelijke analyse van het privacy-risico doorvoert, voorafgaand aan de eindbeslissing over het risico, door middel van het verstrekken van advies en zijn bijstand als adviseur.

Over het *resultaat van de risicobeoordeling*, dat een eindbeslissing is genomen door de vertegenwoordigers binnen het team of departement dat verantwoordelijk is voor de geaffecteerde diensten of klanten, wordt de functionaris voor gegevensbescherming enkel geïnformeerd, niet geconsulteerd. Dit stemt overeen met artikel 38.1 juncto artikel 39.1. a) AVG die vereist dat de functionaris voor gegevensbescherming adviserend dient op te treden ten aanzien van de verwerkingsverantwoordelijke, maar niet medeverantwoordelijk is voor de eindbeslissing. De Geschillenkamer bevestigt op basis daarvan dat het dat de functionaris voor gegevensbescherming enkel over de eindbeslissing omtrent het risico wordt geïnformeerd.

De Geschillenkamer besluit dat enerzijds de verweerder de positie van de functionaris voor de gegevensbescherming op onjuiste wijze interpreteert, maar dat enerzijds aannemelijk is dat in de praktijk de functionaris voor de gegevensbescherming in voldoende mate wordt betrokken. Derhalve kan **geen inbreuk op artikel 38.1 AVG** kan worden vastgesteld.

Voor wat betreft de vaststelling van de Inspectiedienst dat er een **belangenconflict** is in hoofde van de functionaris voor gegevensbescherming doordat hij ook verantwoordelijk is voor compliance, risk management en interne audit, voert de verweerder aan dat in de uitoefening van elk van deze functies de betrokken persoon zelf geen beslissingen neemt, maar zijn rol louter adviserend is. Er zouden bovendien intern de nodige maatregelen zijn genomen om het risico van belangenconflicten te vermijden. Deze maatregelen werden geformaliseerd in een DPO Charter dat door het Audit comité van de verweerder werd gevalideerd op 29 juli 2019.

De Geschillenkamer onderzocht tijdens de hoorzitting de impact die de functionaris voor gegevensbescherming heeft op de besluitvorming uit hoofde van zijn andere functies. Aangaande de rol van de functionaris voor gegevensbescherming werpt de Geschillenkamer op hoe dit verenigbaar is met de functie om interne audits te doen waarbij in een verslag bepaalde elementen kunnen worden vastgelegd die desgevallend tot ontslag van een bepaalde werknemer kunnen leiden. In dit kader is het van belang te weten of de functionaris voor gegevensbescherming die ook de functie bekleedt van hoofd van Interne Audit in die hoedanigheid ook beslissingsrecht heeft.

De Geschillenkamer benadrukt dat er een verschil is tussen louter processen analyseren en via interne audit het functioneren van werknemers beoordelen, hetwelk op gespannen voet staat met de vertrouwensfunctie die de functionaris voor gegevensbescherming heeft binnen de onderneming. De verweerder stelt daaromtrent dat er zich geen probleem van verenigbaarheid stelt omdat de betrokken

functionaris voor gegevensbescherming als hoofd van Interne Audit geen individuele beslissingen treft omtrent werknemers, noch deze beoordeelt.

De Geschillenkamer stelt vast dat de verweerder in zijn conclusie uitgebreid ingaat op de onafhankelijkheid en de adviserende rol van elk van de drie departementen, namelijk het Compliance departement, Interne Audit departement en Risk Management departement, ten aanzien van de overige afdelingen van het bedrijf. Zo stelt de verweerder dat de Audit, Compliance en Risk rollen slechts beperkte risico's van belangenconflicten inhouden, omdat zij "adviserende" functies hebben en geen beslissingsbevoegdheid hebben met betrekking tot verwerkingsactiviteiten Dit brengt de verweerder tot de stelling dat de functionaris voor gegevensbescherming geen taken (ook via zijn functies in elk van de departementen) heeft waardoor hij beslissingen zou kunnen nemen over het doel en de middelen van enige verwerking van persoonsgegevens. [5]

De Geschillenkamer is van oordeel dat daarmee niet is aangetoond dat de functionaris voor gegevensverwerking die deel uitmaakt van elk van deze departementen en daarin een verantwoordelijke positie bekleedt geen taken uitvoert die onverenigbaar zijn met zijn positie als functionaris voor gegevensverwerking.

De Geschillenkamer merkt aldus op dat de onafhankelijkheid en adviserende rol van het departement als dusdanig niet zonder meer kan worden doorgetrokken naar de persoon die tegelijkertijd de functie van functionaris voor gegevensbescherming én verantwoordelijke van een departement vervult.

De Geschillenkamer dient te beoordelen hoe en in welke mate de onafhankelijkheid van de functionaris voor gegevensbescherming ten aanzien van elk van deze drie departementen wordt verzekerd, in het bijzonder in een situatie als de onderhavige waarin de functionaris voor gegevensbescherming niet alleen deel uitmaakt van, maar ook de rol opneemt van verantwoordelijke voor deze departementen.

Immers, de verweerder stipuleert uitdrukkelijk dat naast de verantwoordelijkheden als functionaris voor gegevensverwerking diezelfde persoon eveneens verantwoordelijk is voor compliance, risk management en interne audit.[6] De verweerder duidt aldus zelf eenzelfde fysieke persoon aan als verantwoordelijke voor elk van de drie departementen én als functionaris voor gegevensbescherming. Deze verantwoordelijkheid voor elk van deze drie departementen houdt onmiskenbaar in dat die persoon in die hoedanigheid de doelstellingen van en de middelen voor de verwerking van persoonsgegevens binnen deze drie departementen bepaalt en dus verantwoordelijk is voor de gegevensverwerkingsprocessen die vallen onder het domein compliance, risk management en interne audit zoals werd vastgesteld in het inspectieverslag.

---

[5] Conclusie verweerder, nr. 166 en 167.

[6] Zie brief d.d. 3 april 2019 aan de GBA, die wordt geciteerd in de conclusie.

De Richtlijnen van de Groep 29 voor functionarissen voor gegevensbescherming[7] leggen uit dat de functionaris voor gegevensbescherming binnen de organisatie geen functie kan bekleden waarbij hij of zij de doelstellingen van en de middelen voor de verwerking van persoonsgegevens moet bepalen. Dit is aldus een wezenlijk belangenconflict. De rol van verantwoordelijke van een departement valt aldus niet te rijmen met de functie van functionaris voor gegevensbescherming die zijn taken onafhankelijk moet kunnen uitvoeren. Door het cumuleren in hoofde van eenzelfde fysieke persoon van de functie van verantwoordelijke voor elk van de drie betreffende departementen afzonderlijk enerzijds en de functie van functionaris voor gegevensbescherming anderzijds, ontbreekt voor elk van deze drie departementen enig mogelijk onafhankelijk toezicht vanwege de functionaris voor gegevensbescherming. Bovendien kan het cumuleren van deze functies ertoe leiden dat de geheimhouding en vertrouwelijkheid jegens personeelsleden overeenkomstig artikel 38.5 AVG in onvoldoende mate kan worden gegarandeerd. De Geschillenkamer is bijgevolg van oordeel dat de **inbreuk op artikel 38.6 AVG** is bewezen.

Het is belangrijk dat de functionaris voor gegevensbescherming zijn taken en plichten kan vervullen met respect voor de positie zoals artikel 38 AVG die aan hem heeft toebedeeld, inzonderheid dat hij kan optreden zonder dat er sprake is van een belangenconflict. De Geschillenkamer draagt de verweerder dan ook op om de verwerking op dit punt in overeenstemming te brengen met artikel 38.6 AVG en er aldus voor zorgt dat deze taken of plichten niet tot een belangenconflict leiden.

---

[7] *Krachtens artikel 38, lid 6, kunnen functionarissen voor gegevensbescherming "andere taken en plichten vervullen". Daartoe moet de organisatie er echter voor zorgen dat "deze taken of plichten niet tot een belangenconflict leiden".*
Het uitblijven van een belangenconflict hangt nauw samen met de vereiste om autonoom te handelen. Hoewel functionarissen voor gegevensbescherming andere functies kunnen bekleden, kunnen hen alleen andere taken en plichten worden toevertrouwd als deze geen aanleiding geven tot enig belangenconflict. Dit houdt met name in dat de functionaris voor gegevensbescherming binnen de organisatie geen functie kan bekleden waarbij hij of zij de doelstellingen van en de middelen voor de verwerking van persoonsgegevens moet bepalen. Gezien de specifieke organisatiestructuur van elke organisatie moet dit geval per geval worden beoordeeld.
Als vuistregel worden binnen de organisatie als functies met een belangenconflict beschouwd: functies in het hogere management (bv. Chief Executive, Chief Operating, Chief Financial, Chief Medical Officer, hoofd van de marketingafdeling, hoofd van Human Resources of hoofd van de IT-afdeling), maar ook lagere functies binnen de organisatiestructuur als deze personen de doelstellingen van en middelen voor de verwerking van gegevens moeten bepalen. Daarenboven kan een belangenconflict zich bijvoorbeeld ook voordoen wanneer aan een externe functionaris voor gegevensbescherming wordt gevraagd om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in de rechtbank bij rechtszaken over problemen met de gegevensbescherming.
Afhankelijk van de activiteiten, de grootte en de structuur van de organisatie kan het voor verwerkingsverantwoordelijken of verwerkers een goede praktijk zijn om:

- *de posities te identificeren die incompatibel kunnen zijn met de functie van functionaris voor gegevensbescherming;*
- *interne regels daartoe op te stellen om belangenconflicten te vermijden;*
- *een meer algemene uitleg over belangenconflicten op te nemen;*
- *te verklaren dat hun functionaris voor gegevensbescherming geen belangenconflict heeft in zijn functie als functionaris voor gegevensbescherming, als een manier om anderen voor deze vereiste te sensibiliseren;*
- *in het huisreglement van de organisatie waarborgen op te nemen en ervoor te zorgen dat de vacature voor de positie van functionaris voor gegevensbescherming of de dienstverleningsovereenkomst voldoende gepreciseerd en gedetailleerd is om belangenconflicten te vermijden. In dit verband moeten we rekening houden met het feit dat belangenconflicten diverse vormen kunnen aannemen, afhankelijk van het feit of de functionaris voor gegevensbescherming intern of extern is gerekruteerd.*

WP243Rev01, para 3.5, onderstreping door Geschillenkamer.

Rekening houdend met het feit dat de AVG een sleutelrol heeft toebedeeld aan de functionaris voor gegevensbescherming door hem een informerende en adviserende taak te geven ten aanzien van de verwerkingsverantwoordelijke omtrent alle aangelegenheden die verband houden met de bescherming van persoonsgegevens, waaronder de melding van gegevensinbreuken, gaat de Geschillenkamer eveneens over tot het opleggen van een administratieve geldboete.

Naast de corrigerende maatregel om de verwerking in overeenstemming te brengen met artikel 38.6 AVG, beslist de Geschillenkamer ook tot het opleggen van een administratieve geldboete die er niet toe strekt om een gemaakte overtreding te beëindigen, maar wel met het oog op een krachtige handhaving van de regels van de AVG. Zoals blijkt uit Overweging 148, verlangt de AVG dat bij serieuze inbreuken straffen, met inbegrip van administratieve geldboeten, , naast of in plaats van passende maatregelen die worden opgelegd.[8] De Geschillenkamer doet dit in toepassing van artikel 58.2 i) AVG. Het instrument van administratieve boete heeft dus geenszins tot doel inbreuken te beëindigen. Daartoe voorzien de AVG en de WOG in een aantal corrigerende maatregelen, waaronder de bevelen genoemd in artikel 100, §1, 8° en 9° WOG.

Allereerst wordt de aard en de ernst van de inbreuk door de Geschillenkamer in aanmerking genomen om het opleggen van deze sanctie en de hoogte ervan te rechtvaardigen.

Hierbij stelt de Geschillenkamer vast dat ofschoon er geen element is waaruit blijkt dat er sprake is van een opzettelijke inbreuk, er sprake is van ernstige nalatigheid in hoofde van de verweerder. Hoewel de functionaris voor gegevensbescherming een functie is die in de AVG voor het eerst verplicht op Europees niveau werd voorgeschreven, is het concept van een functionaris voor de gegevensbescherming niet nieuw en bestaat reeds lang in veel lidstaten en in veel organisaties.[9]

Bovendien heeft de Groep 29 reeds op 13 december 2016 richtlijnen vastgesteld voor deze functionarissen. Deze richtsnoeren werden na een wijde publieke consultatie op 5 april 2017 herzien. Zoals blijkt uit het hieronder gestelde zijn deze richtsnoeren duidelijk omtrent de mate waarin de functionaris voor gegevensbescherming ook andere functies kan vervullen binnen de onderneming,

---

[8] Overweging 148 bepaalt: "Met het oog op een krachtiger handhaving van de regels van deze verordening dienen straffen, met inbegrip van administratieve geldboeten, te worden opgelegd voor elke inbreuk op de verordening, naast of in plaats van passende maatregelen die door de toezichthoudende autoriteiten ingevolge deze verordening worden opgelegd. Indien het gaat om een kleine inbreuk of indien de te verwachten geldboete een onevenredige last zou berokkenen aan een natuurlijk persoon, kan in plaats van een geldboete worden gekozen voor een berisping. Er dient evenwel rekening te worden gehouden met de aard, de ernst en de duur van de inbreuk, met het opzettelijke karakter van de inbreuk, met schadebeperkende maatregelen, met de mate van verantwoordelijkheid, of met eerdere relevante inbreuken, met de wijze waarop de inbreuk ter kennis van de toezichthoudende autoriteit is gekomen, met de naleving van de maatregelen die werden genomen tegen de verwerkingsverantwoordelijke of de verwerker, met de aansluiting bij een gedragscode en met alle andere verzwarende of verzachtende factoren. Het opleggen van straffen, met inbegrip van administratieve geldboeten, moet onderworpen zijn aan passende procedurele waarborgen overeenkomstig de algemene beginselen van het Unierecht en het Handvest, waaronder een doeltreffende voorziening in rechte en een eerlijke rechtsbedeling.

[9] Zie onder meer WP243Rev01, para 1.

rekening houdend met de organisatiestructuur eigen aan elke organisatie en geval per geval dient te worden beoordeeld.

Kortom, naar het oordeel van de Geschillenkamer bestaat er geen twijfel dat het cumuleren van de functie van functionaris voor gegevensverwerking met een functie als hoofd van een departement waarop de functionaris voor gegevensverwerking toezicht moet uitoefenen, niet kan gebeuren op een onafhankelijke wijze.

Van een organisatie als van verweerder mag worden verwacht dat het zich op zorgvuldige wijze op de invoering van de AVG voorbereidt en reeds vanaf het tijdstip van de inwerkingtreding van de AVG, overeenkomstig art. 99 AVG in mei 2016. De verwerking van persoonsgegevens is immers een kernactiviteit van verweerder, die bovendien op zeer grote schaal persoonsgegevens verwerkt, waaronder persoonsgegevens die een grote mate van gevoeligheid kunnen hebben voor betrokkenen, onder meer omdat ze een regelmatige en stelselmatige observatie mogelijk maken.[10]

Ook de duur van de inbreuk wordt in beschouwing genomen. De functionaris voor gegevensbescherming is gecreëerd in de AVG die van toepassing is sinds 25 mei 2018, zodat de inbreuk op artikel 38.6 AVG reeds vanaf die datum vaststaat. In ieder geval duurde de overtreding nog voort op de datum van de hoorzitting, i.e. 14 februari 2020.

Tot slot verwerkt verweerder persoonsgegevens van miljoenen mensen. Ondoeltreffende waarborgen voor de bescherming van persoonsgegevens, meer bepaald door de aanwijzing van een functionaris voor gegevensbescherming die niet voldoet aan de vereiste van onafhankelijkheid en dus niet vrij van enig belangenconflict kan optreden, hebben dus een potentiële impact op miljoenen betrokkenen.

Het geheel van de hierboven uiteengezette elementen rechtvaardigt een doeltreffende, evenredige en afschrikkende sanctie als bedoeld in artikel 83 AVG, rekening houdend met de daarin bepaalde beoordelingscriteria, ter hoogte van een bedrag van 50.000 EUR. De Geschillenkamer wijst erop dat de andere criteria van artikel 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.

e) Publicatie van de beslissing

[10] Verwezen zij onder meer naar art. 37.1. AVG. Zie in dit verband ook de rechtspraak van het Europees Hof van Justitie over het potentieel gevoelige karakter van telecommunicatiegegevens, zoals bijv. gevoegde zaken C-293/12 en C-594/12, Digital Rights Ireland en Seitlinger e.a., ECLI:EU:C:2014:238, para 37.

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 100, §1, 9° WOG, de verweerder te **bevelen dat de verwerking in overeenstemming wordt gebracht** met artikel 38.6 AVG. Hiervoor geeft de Geschillenkamer de verweerder een termijn van drie maanden en verwacht de Geschillenkamer dat de verweerder haar rapporteert tegen uiterlijk 31 juli 2020 omtrent het in overeenstemming brengen van de verwerking met voormelde bepalingen;
- op grond van artikel 100, §1, 13° WOG en artikel 101 WOG een **administratieve geldboete** op te leggen van 50.000 EUR.

Tegen deze beslissing kan op grond van artikel 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