Geschillenkamer

Beslissing ten gronde 22/2020 van 8 mei 2020

Dossiernummer : DOS-2018-02716

Betreft : Inbreuk in verband met persoonsgegevens en verplichting tot het (tijdig) sluiten van een verwerkersovereenkomst

De Geschillenkamer van de Gegevensbeschermingsautoriteit, samengesteld uit de heer Hielke Hijmans, voorzitter, en de heren Frank De Smet en Dirk Van Der Kelen, 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 Y, hierna "de verweerder".

1. Feiten en procedure

1. Op 4 juni 2018 maakt de functionaris voor gegevensbescherming van de verweerder op grond van artikel 114/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie en overeenkomstig de verordening 611/2013 van de Europese Commissie[1] bij de Gegevensbeschermingsautoriteit melding van een gegevenslek.

2. Op 6 juni 2018 dient de verweerder hieromtrent een aanvullende kennisgeving in bij de Gegevensbeschermingsautoriteit.

3. In zijn kennisgeving vermeldt verweerder dat hij op 28 mei 2018 telefonisch op de hoogte werd gebracht van het desbetreffende gegevenslek door het federale *Computer Emergency Response Team* (hierna "CERT") en dat deze melding van het CERT schriftelijk werd bevestigd op 29 mei 2018.

Het gegevenslek vond plaats in het kader van de *Master IT Service Agreement* afgesloten op 17 juni 2014 tussen verweerder en de vennootschap naar Indisch recht *Z (*hierna "de verwerker").

Deze laatste werd door middel van deze overeenkomst onder meer aangesteld voor de omvorming van de bestaande e-shop van verweerder, functionerend op basis van het *content management* systeem Drupal 6, naar een nieuwe e-shop functionerend op Magento. Verder werd de verwerker eveneens gevraagd om bestaande productieproblemen betreffende de website te analyseren en te verhelpen.

Voor het testen van de nieuwe e-shop en het verhelpen van deze problemen, plaatste de verwerker een kopie van de productiedatabank met de historiek van bestellingen op een Amazon Web Server (AWS) Cloud. Verwerker activeerde een webserver op poort 80 (HTTP) op deze AWS en maakte daartoe vrije toegang mogelijk door verkeerde veiligheidsinstellingen toe te passen. Bovendien activeerde verwerker de dienst "*Directory Listing*" op deze server, waardoor mogelijk werd gemaakt door de hele directorystructuur op de webserver te browsen.

[1] Verordening (EU) nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie, PB L 173/2.

Hierdoor waren de persoonsgegevens van klanten van verweerder van 22 maart 2018 tot en met 28 mei 2018 toegankelijk vanop het internet. Uit forensische analyse van de logbestanden bleek dat de gegevens door derden geconsulteerd en/of gedownload werden.

Volgens de informatie opgenomen in het door verweerder bij de Gegevensbeschermingsautoriteit ingediende meldingsformulier betrof het meer bepaald identificatiegegevens (naam, adres, telefoonnummer), elektronische identificatiegegevens (IP-adressen), rijksregisternummers en IBAN-nummers van de betrokken personen. Verweerder geeft in dit meldingsformulier tevens aan dat het gegevenslek betrekking heeft op de persoonsgegevens van 32.153 personen.

4. Per e-mail van 6 juni 2018 stelt de Gegevensbeschermingsautoriteit, na overleg met het Belgisch Instituut voor Postdiensten en Telecommunicatie (hierna "BIPT"), verweerder een aantal bijkomende vragen met betrekking tot het gegevenslek en meer bepaald betreffende de aard van dit gegevenslek, de door verweerder gehanteerde risicobeoordelingsmethode, de rechtsgrond van de verwerking, de kennisgeving aan de betrokkenen en de eventuele betrokkenheid van andere Europese lidstaten en toezichthoudende autoriteiten.

5. Per e-mail van 11 juni 2018 beantwoordt de functionaris voor gegevensbescherming van verweerder een aantal van de hierboven vermelde vragen.

Verweerder maakt een ontwerp van kennisgeving naar de betrokkenen over alsook een ontwerp van persbericht. Verder preciseert verweerder dat verwerker geen toestemming had om de gegevens te kopiëren naar een niet-productieomgeving. De verweerder deelt eveneens mee dat geen andere Europese gegevensbeschermingsautoriteiten werden geïnformeerd.

6. Per e-mail van 12 juni 2018 stelt de Gegevensbeschermingsautoriteit enkele bijkomende vragen aan verweerder.

Deze verzoekt verweerder meer bepaald een kopie van de verwerkersovereenkomst over te maken alsook de resultaten van de veiligheidsaudit uitgevoerd ten aanzien van de verwerker. Verder vraagt de Gegevensbeschermingsautoriteit of een gegevensbeschermingseffectbeoordeling zal worden uitgevoerd met betrekking tot de risico's verbonden aan het beheer van de e-shops van verweerder en of nieuwe concrete afspraken werden gemaakt met de verwerker.

7. Per e-mail van 14 juni 2018 beantwoordt de functionaris voor gegevensbescherming van verweerder deze vragen.

8. Op 11 juli 2018 beslist het Directiecomité van de Gegevensbeschermingsautoriteit op grond van artikel 63, 1° WOG om het dossier aanhangig te maken bij de inspectiedienst aangezien het ernstige aanwijzingen vaststelt betreffende het bestaan van een inbreuk op, enerzijds, de verantwoordingsplicht inzake de beoordeling van het risico bij de melding van een inbreuk in verband met persoonsgegevens en, anderzijds, de verplichting om (tijdig) een verwerkersovereenkomst te sluiten.

9. Per e-mail van 10 augustus 2018 maakt de functionaris voor gegevensbescherming van verweerder de antwoorden van verweerder op de vragen gesteld door de Gegevensbeschermingsautoriteit op 10 juli 2018 over.

10. Per brief van 5 februari 2019 stelt de Gegevensbeschermingsautoriteit een aantal bijkomende vragen aan verweerder.

11. Op 22 februari 2019 maakt de functionaris voor gegevensbescherming van verweerder de antwoorden van verweerder op de vragen gesteld door de Gegevensbeschermingsautoriteit op 5 februari 2019 over.

12. Op 12 augustus 2019 maakt de Inspectiedienst overeenkomstig artikel 91, §2 WOG zijn inspectieverslag over aan de voorzitter van de Geschillenkamer.

13. Op 12 september 2019 beslist de Geschillenkamer op grond van de artikelen 95, §1, 1°, en 98 WOG dat de klacht gereed is voor behandeling ten gronde.

14. Per aangetekende brief van 12 september 2019 wordt verweerder in kennis gesteld van het feit dat de klacht gereed is voor behandeling ten gronde en wordt deze tevens op grond van artikel 99 WOG in kennis gesteld van de termijn om zijn verweermiddelen in te dienen.

15. Op 14 oktober 2019 legt verweerder zijn conclusies neer en verzoekt deze op grond van artikel 98, 2° WOG om gehoord te worden.

16. Op 8 april 2020 wordt de verweerder overeenkomstig artikel 53 van het reglement van interne orde gehoord door de Geschillenkamer.

17. Op 23 april 2020 wordt overeenkomstig artikel 54 van het reglement van interne orde het proces-verbaal van de hoorzitting aan de verweerder overgemaakt.

18. Op 28 april 2020 maakt de verweerder zijn opmerkingen over, die overeenkomstig artikel 54, lid 2 van het reglement van interne orde als bijlage bij het proces-verbaal van verhoor worden gevoegd.

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

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

Artikel 24.1 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."

Artikel 28.3 AVG

"3. De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Die overeenkomst of andere rechtshandeling bepaalt met name dat de verwerker:

a) de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt;
b) waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;
c) alle overeenkomstig artikel 32 vereiste maatregelen neemt;
d) aan de in de leden 2 en 4 bedoelde voorwaarden voor het in dienst nemen van een andere verwerker voldoet;
e) rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III vastgestelde rechten van de betrokkene te beantwoorden;
f) rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36;
g) na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht;
h) de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk maakt en eraan bijdraagt. 4.5.2016 L 119/49 Publicatieblad van de Europese Unie NL
Waar het gaat om de eerste alinea, punt h), stelt de verwerker de verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op deze verordening of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming."

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 AVG

"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.
2. De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen.
3. De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:
a) de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
b) de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
c) de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

4. Indien de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de toezichthoudende autoriteit, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke daartoe verplichten of besluiten dat aan een van de in lid 3 bedoelde voorwaarden is voldaan."

3. Motivering

3.1. Wat betreft de vaststellingen inzake de verantwoordingsplicht en de verantwoordelijkheid van verweerder (artikelen 5, 24, 32, 33 en 34 AVG)

Vaststellingen inspectieverslag

19. In zijn inspectieverslag stelt de Inspectiedienst vast dat verweerder "*geen verantwoording verschaft over hoe het komt tot een concrete risico-gebaseerde benadering die wordt opgelegd door (onder meer) artikelen 5, 24, 32, 33 en 34 van de AVG. De verwijzingen door [verweerder] naar "De ENISA methode voor een gegevenslek" en naar "De CNIL methode voor een DPIA" zijn zeer algemeen van aard en vaag, waardoor [verweerder] voor dit dossier niet heeft gehandeld in overeenstemming met artikel 5, lid 2 en artikel 24, lid 1 van de AVG*".

Verweermiddelen verweerder

20. Met betrekking tot deze vaststelling van de Inspectiedienst stelt verweerder dat hij afleidt uit de samenlezing van de hierboven vermelde bepalingen dat deze tenlastelegging ten eerste betrekking heeft op de verplichting tot het uitvoeren van een gegevensbeschermingseffectbeoordeling in de zin van artikel 35 AVG en argumenteert deze dat hij voor de betroffen verwerking zijns inziens niet verplicht was over te gaan tot het uitvoeren van een dergelijke beoordeling noch tot enige andere risicobeoordeling.

21. Hij stelt wat dit betreft vooreerst dat de handeling die aanleiding gaf tot het gegevenslek plaatsvond *vóór* de datum van toepassing van de AVG en bijgevolg artikel 35 AVG, dat het concept van de gegevensbeschermingseffectbeoordeling introduceert.

22. Ten tweede wijst verweerder erop dat de verplichting een dergelijke effectbeoordeling uit te voeren enkel van toepassing is wanneer de verwerking een waarschijnlijk hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Hij stelt dat *in casu* de door de verwerker uitgevoerde verwerkingsactiviteit die aan de grondslag lag van het gegevenslek evenwel uitdrukkelijk door verweerder werd verboden. Verweerder verduidelijkt dat de verwerker voor het testen en ontwikkelen van software een niet-productieomgeving gebruikte waarin deze uitsluitend geanonimiseerde

gegevens mocht gebruiken. Verweerder besluit dat bijgevolg niet van hem kon worden verwacht een risicobeoordeling uit te voeren betreffende een activiteit van zijn verwerker waarvan hij niet op de hoogte was en waarvoor hij het gebruik van persoonsgegevens contractueel had verboden.

Verweerder verwijst in dit verband naar de Bijlage C035A2 genaamd "*Data Privacy Requirements*" bij de in 2014 tussen de partijen gesloten *Master IT Service Agreement* die een clausule bevatte die stelde dat "*vertrouwelijke gegevens [niet] mogen worden gekopieerd van een productieomgeving naar een niet-productieomgeving, tenzij de vertrouwelijke gegevens worden gemaskeerd*". Hij verwijst eveneens naar artikel 7 van de later tussen de partijen afgesloten verwerkersovereenkomst, dat onder meer stelt: "*De aanbieder is verplicht om bij de verwerking van Persoonsgegevens (…): r) Persoonsgegevens in niet-productieomgevingen anoniem te maken met behulp van industriestandaardtechnologie die nog steeds de ontwikkeling, het testen en de aanvaarding bij Aanbieders of [verweerder] mogelijk maakt*".

23. Verweerder benadrukt eveneens dat hij de verwerker naar aanleiding van het gegevenslek op 15 juni 2018 formeel in gebreke stelde en voegt hiervan het bewijs bij.

24. Verder stelt verweerder met betrekking tot dit deel van de tenlastelegging dat hij wel degelijk de passende en organisatorische maatregelen nam om risico's te beoordelen en een passend beveiligingsniveau te waarborgen om zulke risico's te voorkomen. Hij stelt dat in de voornoemde Bijlage C035A2 bij de overeenkomst gesloten op 17 juni 2014 met verwerker een overzicht bevatte van de risico's met betrekking tot de verwerking van persoonsgegevens, de belangrijkste mechanismen om persoonsgegevens te beschermen alsook de verplichtingen van de verwerker in dit verband.

25. Verweerder wijst erop dat overeenkomstig artikel 6.2 van de hierboven vermelde bijlage bovendien jaarlijkse audits van de verwerker werden voorzien en voegt de laatste twee auditrapporten, opgesteld door *Ernst & Young LLP*, als bewijsstukken bij.

26. Tot slot argumenteert verweerder dat hij wel degelijk beschikt over een risicobeoordelingsmethode voor datalekken, en dat dit zowel het geval was ten tijde van als na het gegevenslek van 2018. Hij verwijst hierbij naar zijn "*Data Breach Severity Assessment Method",* gebaseerd op de ENISA-methode, aangevuld met onder meer ISO 31000 en ISO 27005 en voegt hiervan documentatie toe aan zijn conclusie van antwoord. Verweerder stelt dat deze, naast deze risicobeoordelingsmethode voor gegevenslekken, eveneens beschikt over een algemene risicobeoordelingsmethode. Hij verwijst wat dit betreft naar zijn interne "*Security Risk Management Policy*", die wordt gebruikt om de risico's inherent aan alle verwerkingsactiviteiten te beoordelen. Verweerder voegt hieromtrent documentatie

toe alsook een voorbeeld van een analyse op basis van deze methode, daterend van 16 september 2017.

27. Verweerder voegt hieraan toe dat op basis van de hierboven vermelde beoordelingsmethodiek ook de risico's verbonden aan het gegevenslek dat aanleiding gaf tot de aanhangigmaking van dit dossier werd ingeschat. Hij preciseert dat bij deze procedure achtereenvolgens (het team van) de functionaris voor gegevensbescherming, de *security manager* en de *chief compliance officer* werden betrokken bij deze risicobeoordeling, waarna hun analyse werd goedgekeurd door het directiecomité van verweerder.

28. Verweerder benadrukt tijdens de hoorzitting dat zowel hijzelf als de Gegevensbeschermingsautoriteit in dit dossier tot de conclusie kwamen dat het risico van het gegevenslek als hoog diende te worden ingeschat, en dat verweerder alle nodige maatregelen nam in dit verband[2] en deze bijgevolg niet begrijpt waarop de tenlastelegging betreffende de niet-naleving van de verantwoordingsplicht is gesteund.

Analyse Geschillenkamer

29. De Geschillenkamer wijst er op dat de verantwoordingsplicht van artikel 5.2 AVG één van de centrale pijlers van de AVG vormt en inhoudt dat op de verwerkingsverantwoordelijke de verantwoordelijkheid 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.[3]

Dit blijkt onder meer uit het Advies 3/2010 betreffende het "verantwoordingsbeginsel" van de Groep 29, waarin deze stelt dat twee aspecten moeten worden benadrukt met betrekking tot 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*".[4]

---

[2] Met name de melding en aanvullende melding bij de Gegevensbeschermingsautoriteit, het van een persbericht en van individuele meldingen aan alle betrokkenen.

[3] DOCKSEY, C., "Article 24. Responsibility of the controller" in KUNER, C., BYGRAVE, L.A. en DOCKSEY, C. (eds.), *The EU General Data Protection Regulation: A Commentary,* Oxford University Press, 2020, (508)557: "*The principle of accountability is one of the central pillars of the GDPR and one of its most significant innovations. It places responsibility firmly on the controller to take proactive action to ensure compliance and to be ready to demonstrate that compliance*".

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

30. Deze verantwoordingsplicht heeft niet enkel betrekking op de bepalingen van artikel 5.1 AVG, doch betreft de gehele AVG.

31. Het voormelde vloeit voort uit de samenlezing van artikel 5.2 AVG en artikel 24.1 AVG, dat stelt dat "*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".*

32. De Geschillenkamer wijst erop 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.[5]

33. In zijn Advies 3/2010 neemt de Groep 29 een niet-exhaustieve lijst op van "verantwoordingsmaatregelen" die verwerkingsverantwoordelijken kunnen treffen teneinde aan deze verplichting te voldoen. De Groep 29 verwijst hierbij onder meer naar: het vaststellen van interne procedures, het opstellen van een schriftelijk en bindend beleid betreffende gegevensbescherming, het aanstellen van een functionaris voor gegevensbescherming, het ontwikkelen van interne procedures voor het doeltreffend beheren en rapporteren van inbreuken op de beveiliging.[6]

34. Wat betreft de evaluatie van de doeltreffendheid van deze maatregelen, verwijst de Groep 29 naar het uitvoeren van interne en/of externe audits als *best practice*. Deze preciseert hierbij dat de controlemethoden voor de beoordeling van de doeltreffendheid van de genomen maatregelen dienen te worden afgestemd op de specifieke risico's die de gegevensverwerking met zich meebrengt, de hoeveelheid te verwerken gegevens en de gevoeligheid van deze gegevens.[7]

35. Tot slot dient erop de worden gewezen dat transparantie een integraal deel uitmaakt van de verantwoordingsplicht en dat deze transparantie ten opzichte van de toezichthoudende autoriteiten alsook ten aanzien van de betrokkenen en het bredere publiek de verwerkingsverantwoordelijke in een sterkere positie plaatst wat betreft zijn verantwoordingsplicht.[8]

---

[5] FOCQUET, A. en DECLERCK, E., *Gegevensbescherming in de praktijk*, Intersentia, 2019, 64.

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

[7] Idem, p. 17-18.

[8] Idem, p. 16.

36. De Geschillenkamer oordeelt dat verweerder op basis van de neergelegde stukken alsook zijn verweer aantoont dat deze overeenkomstig artikel 24.1 AVG *in casu* de nodige passende technische en organisatorische maatregelen nam en overeenkomstig artikel 5.2 AVG op verzoek van de Gegevensbeschermingsautoriteit eveneens aantoonde dergelijke maatregelen te hebben getroffen.

Verweerder toont meer bepaald aan dat hij:

- in zijn contracten met de verwerker - zowel in de in 2014 gesloten *Master IT Service Agreement* als in de na de inwerkingtreding van de AVG gesloten verwerkersovereenkomst - de nodige bepalingen opnam teneinde de verwerking van persoonsgegevens door de verwerker te regelen, en meer bepaald de verwerking van persoonsgegevens voor doeleinden van ontwikkeling en *testing* van software door deze laatste te verbieden (in het bijzonder in de Bijlage C035A2 gevoegd bij de Master IT Service Agreement en in artikel 7 van de op 6 juni 2018 afgesloten verwerkersovereenkomst);

- de nodige interne risicobeoordelingsmethoden heeft uitgewerkt en gedocumenteerd, zowel wat betreft gegevenslekken (de "*Data Breach Severity Assessment Method")* als wat betreft de beoordeling van risico's inherent aan *alle* verwerkingsactiviteiten *("Security Risk Management Policy"*) en deze documentatie alsook een toepassingsvoorbeeld van deze methodiek overmaakte aan de Geschillenkamer;

- de doeltreffendheid van de door hem uitgewerkte procedures en maatregelen evalueert door middel van jaarlijkse externe audits;

- zodra deze in kennis werd gesteld van het gegevenslek door CERT, op transparante wijze handelde zowel ten aanzien van de Gegevensbeschermingsautoriteit als de betrokkenen. Verweerder diende overeenkomstig artikel 33 AVG een meldingsformulier alsook een aanvullende kennisgeving in bij de Gegevensbeschermingsautoriteit op respectievelijk 4 en 6 juni 2018. Verweerder deelde de inbreuk in verband met persoonsgegevens overeenkomstig artikel 34 AVG eveneens mee aan de betrokkenen en publiceerde hieromtrent een persbericht op 15 juni 2018; en

- zijn verwerker formeel in gebreke stelde op 15 juni 2018 naar aanleiding van de verboden verwerking en hiervan het bewijs levert.

37. De Geschillenkamer is om deze redenen van oordeel dat er **geen inbreuk op de artikelen 5.1 f), 5.2, 24.1, 32, 33, 34 en 35 AVG** kan worden vastgesteld.

3.2. Wat betreft de vaststellingen inzake de verplichting om een overeenkomst te sluiten met verwerkers (artikel 28 AVG)

Vaststellingen inspectieverslag

38. In het inspectieverslag overgemaakt door de Inspectiedienst aan de Geschillenkamer op 12 augustus 2019 wordt vastgesteld dat de verweerder "*op het moment van de inbreuk in verband met de persoonsgegevens (in de periode tussen 22/03/2018 en 28/05/2018) geen overeenkomst had afgesloten met de verwerker voor de betrokken verwerkingsactiviteit. De overeenkomst werd slechts afgerond door [verweerder] op 06/06/2018, zoals blijkt uit de datum boven de handtekening van de persoon die ondertekende namens [verweerder]. Bijgevolg heeft [verweerder] voor dit dossier niet gehandeld in overeenstemming met artikel 28 AVG*".

Verweermiddelen verweerder

39. In zijn conclusie van antwoord en tijdens de hoorzitting stelt verweerder in antwoord op deze tenlastelegging dat met verwerker op 17 juni 2014 een allesomvattende *Master IT Service Agreement* werd afgesloten en dat deze overeenkomst in zijn artikel 14.4 uitdrukkelijk de verplichtingen inzake de bescherming van persoonsgegevens vastlegde. Verweerder voegt hieraan toe dat verder Bijlage C035A2 getiteld "*Data Privacy Requirements*", dat integraal deel uitmaakte van de *Master IT Service Agreement*, aanvullende verplichtingen voor verwerker bevatte.[9]

40. Tijdens de hoorzitting d.d. 8 april 2020 wijst verweerder erop dat het op 17 juni 2014 afgesloten contract met verwerker en meer bepaald het artikel 14.4 voldeed aan de voorwaarden die werden opgelegd door de wet van 1992[10], die met name stelde dat er een contract moest bestaan tussen de partijen en dat hierin moest worden voorzien dat de verwerker enkel persoonsgegevens verwerkte op instructie van de verwerkingsverantwoordelijke en niet voor andere doeleinden dan die bepaald door deze laatste.

41. Verweerder voegt hier aan toe dat deze clausule evenwel reeds veel uitgebreider was aangezien deze eveneens bepalingen bevatte over gegevenslekken en bijstand, en zo reeds een aantal elementen bevatte die later wet werden met de AVG.

42. Verder stelt verweerder dat naar aanleiding van de inwerkingtreding van de AVG onderhandelingen plaatsvonden met verwerker en een nieuwe verwerkersovereenkomst werd opgesteld die op 21 mei

[9] Conclusie van antwoord verweerder nr. 57, p. 15.

[10] Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (opgeheven).

2018 werd ondertekend door de verwerker en op 6 juni 2018 door verweerder zelf. Verweerder stelt dat het feit dat de ondertekening van deze overeenkomst door laatstgenoemde slechts een formaliteit uitmaakte en dat het feit dat dit pas gebeurde op 6 juni 2018 irrelevant is aangezien deze overeenkomst enkel verplichtingen bevat voor de verwerker.

Analyse Geschillenkamer

43. Overeenkomstig artikel 28.3 AVG dient de verwerking door een verwerker te worden geregeld in "*een overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven".* Dit artikel lijst eveneens de verplichte vermeldingen op die dergelijke rechtshandeling dient te bevatten[11].

44. De Geschillenkamer stelt vast dat de verwerkersovereenkomst opgesteld door verweerder naar aanleiding van de inwerkingtreding van de AVG de verplichte vermeldingen van artikel 28 AVG bevat, doch dat deze op datum van inwerkingtreding van de AVG niet door verweerder was ondertekend.

45. Van een organisatie als verweerder mag evenwel worden verwacht dat deze zich op zorgvuldige wijze op de invoering van de AVG voorbereidt en dit reeds vanaf het tijdstip van de inwerkingtreding van de AVG, overeenkomstig artikel 99 AVG in mei 2016. De verwerking van persoonsgegevens is immers een kernactiviteit van verweerder, die bovendien op zeer grote schaal dergelijke gegevens verwerkt.

46. Gelet op het feit dat de AVG van toepassing werd vanaf 25 mei 2018 diende de tussen verweerder en zijn verwerker afgesloten verwerkersovereenkomst bijgevolg uiterlijk op deze datum door beide partijen te zijn ondertekend.

47. De Geschillenkamer stelt evenwel vast dat wilsovereenstemming bestond tussen de partijen betreffende deze verwerkersovereenkomst en dat deze voor de datum van inwerkingtreding van de AVG werd opgesteld door verweerder en werd ondertekend door de verwerker.

48. De Geschillenkamer is bijgevolg van oordeel dat *in casu* geen **inbreuk op artikel 28 AVG** dient te worden vastgesteld.

[11] Artikel 28.3, a) - h) AVG.

4. Publicatie van de beslissing

49. Gelet op het belang van transparantie met betrekking tot de besluitvorming van de Geschillenkamer, wordt deze beslissing overeenkomstig artikel 95, §1, 8° WOG gepubliceerd op de website van de Gegevensbeschermingsautoriteit. Het is evenwel niet nodig dat daartoe de identificatiegegevens van de verweerder rechtstreeks worden bekendgemaakt.

OM DEZE REDENEN,

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

- op grond van **artikel 100, §1, 2° WOG** de **buitenvervolgingstelling** te bevelen.

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