



Beslissing ten gronde 183/2022 van 14 december 2022

Dossiernummer : DOS-2022-00365

Betreft : Verstrekking van persoonlijke informatie aan derden zonder toestemming van de betrokkene

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 klager: Mevrouw X, hierna “de klagster”,

De verweerster: Y, vertegenwoordigd door Mr. Heidi Waem en Mr. Simon Verschaeve, kantoorhoudende te 1000 Brussel, Wolstraat 70, hierna “de verweerster”.

I. Feiten en procedure

1. Op 19 januari 2022 dient de klaagster een klacht in bij de Gegevensbeschermingsautoriteit tegen verweerster.

De klaagster deed beroep op de diensten van de verweerster – bij wie zij een rechtsbijstandverzekering had afgesloten - voor de juridische afhandeling van een verkeersongeval waar zij het slachtoffer van werd. In het kader van de regeling van dit schadegeval, heeft de klaagster een raadsman aangesteld. Tussen de verweerster en de raadsman van de klaagster werd correspondentie gevoerd in het kader van een dispuut omtrent de door de klager verzochte tussenkomst van de verweerster in de erelonen en andere kosten voor deze juridische bijstand.

Door een menselijke vergissing stuurde een medewerker op 2 juni 2021 een e-mail met betrekking tot deze bijstand naar een foutief e-mailadres. De e-mail bevatte de volgende gegevens: naam en voornaam van de klaagster, de advocaat van de klaagster, het dossiernummer, betaalde voorschotten, het feit dat de betrokkene een ongeval heeft gehad met letsel tot gevolg, het verloop van het dossier en de betwisting over het feit of Y al dan niet tussen dient te komen als rechtsbijstandsverzekeraar. De e-mail bevatte geen bijlagen.

Op vrijdag 4 juni 2021 werd de DPO van de verweerster door de betrokken medewerker gecontacteerd naar aanleiding van het incident en er werd onmiddellijk een intern onderzoek gestart. Op maandag 7 juni 2021 om 14u58 werd de informatie bekomen die nodig was om de aard van het incident voldoende vast te stellen waarna het intern onderzoek door de bevoegde dienst (Data Protection Unit) om 15u38 werd afgerond. De melding aan de GBA vond diezelfde dag om 21u17 plaats.

De verweerster contacteerde op maandag 7 juni 2021 eveneens de foutieve bestemming met de vraag om de e-mail te vernietigen en de informatie niet verder te delen met derden, door te sturen, op te slaan of op enige wijze te gebruiken.

De klaagster werd vervolgens op dinsdag 8 juni 2021 geïnformeerd over het feit dat een gegevenslek had plaatsgevonden. Tot slot contacteerde verweerster eveneens de raadsman van de klaagster op 9 juni 2021.

2. Op 14 februari 2022 wordt de klacht door de Eerstelijnsdienst ontvankelijk verklaard op grond van de artikelen 58 en 60 WOG en wordt de klacht op grond van artikel 62, §1 WOG overgemaakt aan de Geschillenkamer.
3. Op 11 maart 2022 wordt overeenkomstig artikel 96, §1 WOG het verzoek van de Geschillenkamer tot het verrichten van een onderzoek overgemaakt aan de Inspectiedienst, samen met de klacht en de inventaris van de stukken.

4. Op 14 april 2022 wordt het onderzoek door de Inspectiedienst afgerond, wordt het verslag bij het dossier gevoegd en wordt het dossier door de inspecteur-generaal overgemaakt aan de Voorzitter van de Geschillenkamer (artikel 91, § 1 en § 2 WOG).

Het verslag bevat vaststellingen met betrekking tot het voorwerp van de klacht en besluit :

1. inbreuk op artikel 5, lid 1, a), c) en f) en lid 2, artikel 6, lid 1, artikel 24, lid 1 en artikel 25, lid 1 en lid 2 van de AVG in de kader van de klacht in dit dossier;
2. geen inbreuk in het algemeen op artikel 5, artikel 24, lid 1 en artikel 25, lid 1 en lid 2 AVG;
3. inbreuk op artikel 33 van de AVG en artikel 34 van de AVG.

Het verslag bevat daarnaast vaststellingen die verder gaan dan het voorwerp van de klacht.

De Inspectiedienst stelt, in hoofdlijnen, vast:

4. geen inbreuk op artikel 38, lid 1 en artikel 39 AVG.
5. Op 29 april 2022 beslist de Geschillenkamer op grond van artikel 95, § 1, 1^o en artikel 98 WOG dat het dossier gereed is voor behandeling ten gronde.
6. Op 29 april 2022 worden de betrokken partijen per aangetekende zending in kennis gesteld van de bepalingen zoals vermeld in artikel 95, § 2, alsook van deze in artikel 98 WOG. Tevens worden zij op grond van artikel 99 WOG in kennis gesteld van de termijnen om hun verweermiddelen in te dienen.

Voor wat betreft de vaststellingen met betrekking tot het voorwerp van de klacht werd de uiterste datum voor ontvangst van de conclusie van antwoord van de verweerster vastgelegd op 10 juni 2022, deze voor de conclusie van repliek van de klaagster op 1 juli 2022 en ten slotte deze voor de conclusie van dupliek van de verweerster op 22 juli 2022.

7. Op 29 april 2022 aanvaardt de klaagster elektronisch alle communicatie omtrent de zaak.
8. Op 29 april 2022 aanvaardt de verweerster elektronisch alle communicatie omtrent de zaak.
9. Op 20 mei 2022 vraagt de verweerster een kopie van het dossier (artikel 95, § 2, 3^o WOG), dewelke haar werd overgemaakt op 23 mei 2022.
10. Op 10 juni 2022 ontvangt de Geschillenkamer de conclusie van antwoord vanwege de verweerster voor wat betreft de vaststellingen met betrekking tot het voorwerp van de klacht. Deze conclusie bevat eveneens de reactie van de verweerster omtrent de vaststellingen die door de Inspectiedienst werden gedaan buiten de scope van de klacht. In hoofddorde voert de verweerster aan dat de procedure en de wijze waarop deze gevoerd wordt door de Inspectiedienst en de Geschillenkamer de beginselen van behoorlijk bestuur schendt. In ondergeschikte orde betoogt de verweerster dat deze inbreuk in verband met persoonsgegevens geen inbreuk vormt op de beginselen inzake rechtmatigheid, minimale

gegevensverwerking, integriteit en vertrouwelijkheid van de AVG. Verder heeft de verweerster de AVG niet geschonden naar aanleiding van de melding van het gegevenslek aan de GBA en aan de betrokkene.

11. Op 14 juli 2022 bevestigt de Geschillenkamer aan de verweerster dat geen conclusie van repliek werd ingediend door de klagster voor wat betreft de vaststellingen met betrekking tot het voorwerp van de klacht.
12. Op 20 juli 2022 ontvangt de Geschillenkamer de kennisgeving van de verweerster dat zij geen conclusie van dupliek zal indienen.

II. Motivering

II.1. Beginselen van behoorlijk bestuur

13. De verweerster laat gelden dat zowel de procedure als de wijze waarop deze gevoerd werd door de Geschillenkamer en de Inspectiedienst de beginselen van behoorlijk bestuur schendt. De verweerster houdt voor dat het zorgvuldigheidsbeginsel werd geschonden door de Inspectiedienst en de Geschillenkamer door de wijze waarop de klacht werd onderzocht. De Geschillenkamer zou dit onder meer gedaan hebben door te beslissen dat er in deze zaak een Inspectieonderzoek vereist was. De Inspectiedienst zou deze beginselen geschonden hebben door te beslissen om het toepassingsgebied van het onderzoek verder uit te breiden buiten het voorwerp van de klacht. De verweerster stelt ook dat het redelijkheidsbeginsel en het proportionaliteitsbeginsel geschonden werden. Deze voornoemde uitbreiding van het toepassingsgebied had betrekking op aspecten die in het kader van een ander onderzoek van de Inspectiedienst recent reeds werden bevraagd en onderzocht en waar de Inspectiedienst tot de vaststelling was gekomen dat er geen inbreuk voorlag.
14. Dienaangaande merkt de Geschillenkamer op dat zij inderdaad besloten heeft om de Inspectiedienst te vatten om een onderzoek uit te voeren op basis van artikel 94, 1^e WOG. De Geschillenkamer evalueert in elk dossier zowel wat de potentiële persoonlijke gevolgen voor een klager als de maatschappelijke gevolgen van de litigieuze verwerking zijn. Onderhavige zaak betreft een inbreuk in verband met persoonsgegevens (gegevenslek). Inbreuken in verband met persoonsgegevens vormen een probleem op zich, maar kunnen ook symptomen zijn van een kwetsbaar, mogelijk verouderd gegevensbeveiligingssysteem. Bovendien kunnen deze inbreuken duiden op zwakke plekken in het systeem, die desgevallend moeten worden aangepakt.
15. De Geschillenkamer herinnert eraan dat een klacht zelden een volledig of objectief beeld geeft van een verwerking of situatie die door de klagster aan de kaak gesteld wordt. Aangezien de Geschillenkamer op basis van de klacht niet over alle relevante informatie beschikt omtrent de relevante feiten, heeft zij een Inspectieonderzoek gevraagd. In dit kader benadrukt de Geschillenkamer dat een onderzoek door de Inspectiedienst dus niet altijd

wordt gevraagd met de bedoeling om noodzakelijkerwijs een inbreuk vast te stellen, maar wel om een zo juist mogelijk overzicht van de relevante objectieve feiten te verkrijgen. Het onderzoek door de Inspectiedienst kan net zo goed een inbreuk uitsluiten als vaststellen. Het onderzoek wordt dus à charge en à décharge gevoerd.

16. De verweerster werpt op dat het uit de klacht zelf duidelijk blijkt dat de inbreuk in verband met persoonsgegevens het gevolg is van een menselijke vergissing, en dat dit ook achteraf uit het Inspectieverslag blijkt. Ook al blijkt uit het Inspectieverslag dat de inbreuk in verband met persoonsgegevens *in casu* inderdaad het gevolg was van een menselijke vergissing, wijst de Geschillenkamer erop dat zij dit vooraf niet met volledige zekerheid kon vaststellen en het haar niet verweten kan worden dat zij dus een onderzoek gevraagd heeft om een volledig en juist overzicht te krijgen van de omstandigheden waarin de inbreuk in verband met persoonsgegevens heeft plaatsgevonden. Meer in algemene zin benadrukt de Geschillenkamer dat de beslissing over de opvolging van een dossier overeenkomstig artikel 95, § 1, WOG een noodzakelijke tussenstap is in deze procedure die de Geschillenkamer in alle vrijheid moet kunnen nemen.
17. De verweerster voert eveneens aan dat de Geschillenkamer de klacht had moeten seponeren op basis van haar sepotbeleid, meer bepaald sepotgrond B.3 “Uw klacht is een nevangenschil bij een ruimer geschil dat moet worden beslecht voor hoven en rechtbanken en administratieve rechtscolleges of een andere bevoegde autoriteit”. In dit kader herinnert de Geschillenkamer eraan dat zij niet verplicht is deze klachten te seponeren, maar dat zij de discretionaire bevoegdheid heeft om bij elke klacht individueel te onderzoeken of zij deze zal seponeren of niet. In onderhavige zaak werd besloten om deze klacht niet te seponeren maar heeft de Geschillenkamer beslist om de Inspectiedienst te vatten omwille van de volgende redenen. De verweerster verwerkt in haar hoedanigheid van rechtsbijstandsverzekeraar gevoelige gegevens van betrokkenen. Bovendien verwerkt de verweerster deze gegevens op grote schaal. Het is dus van belang dat voldoende waarborgen, zoals bijvoorbeeld met betrekking tot de vertrouwelijkheid, voorzien worden door de verweerster zodat deze verwerkingen op grote schaal van gevoelige persoonsgegevens overeenkomstig de grondbeginselen van de AVG gebeuren.
18. De Geschillenkamer wenst dit verder te verduidelijken, zonder vooruit te lopen op de beoordeling van de feiten die ten grondslag liggen aan de klacht en de eventuele inbreuken op de AVG die daaruit zouden kunnen voortvloeien. Daartoe verwijst de Geschillenkamer naar artikel 100 WOG¹ waarin haar beslissingsbevoegdheid wordt bepaald in het kader van

¹ Art. 100. §1. De geschillenkamer heeft de bevoegdheid om:

1° een klacht te seponeren;

2° de buitenvervolginstelling te bevelen;

3° de opschorting van de uitspraak te bevelen;

4° een schikking voor te stellen;

5° waarschuwingen en berispingen te formuleren;

een procedure ten gronde. Deze bepaling voorziet uitdrukkelijk dat, naast tal van andere maatregelen, de Geschillenkamer ook in de procedure ten gronde over de mogelijkheid beschikt om een klacht te seponeren (artikel 100, §1, 1° WOG). De Geschillenkamer benadrukt dat het haar vrijstaat om klachten ook in deze fase om technische redenen of om beleidsmatige redenen te seponeren, overeenkomstig de voorwaarden in de rechtspraak van het Marktenhof.²

19. De verweerster stelt ook dat de Inspectiedienst de zorgvuldigheidsplicht geschonden heeft door te beslissen om het toepassingsgebied van het onderzoek verder uit te breiden. Deze uitbreiding van het toepassingsgebied had daarenboven zelfs betrekking op aspecten die in het kader van een ander onderzoek van de Inspectiedienst recent reeds werden bevraagd en onderzocht, en waar de Inspectiedienst tot de vaststelling was gekomen dat er geen inbreuk voorlag. De verweerster voert aan dat om diezelfde redenen ook het redelijkheidsbeginsel en het proportionaliteitsbeginsel geschonden werden. Bovendien is ook het vertrouwensbeginsel ten aanzien van de verweerster geschonden. Het vertrouwensbeginsel of rechtszekerheidsbeginsel houdt immers in dat “het recht voorzienbaar en toegankelijk moet zijn, zodat de rechtzoekende in redelijke mate de gevolgen van een bepaalde handeling kan voorzien op het tijdstip dat de handeling wordt verricht”.³ Daarnaast mag de overheid niet zonder objectieve en redelijke verantwoording van een beleidslijn afwijken, aldus de verweerster.⁴ Verder stelt de verweerster dat ook het gelijkheidsbeginsel en het non-discriminatiebeginsel zoals begrepen in de artikelen 10 en 11 van de Grondwet geschonden werden. Het valt immers niet redelijk te verantwoorden waarom de GBA wel gevolg geeft aan het gegevenslek in voorliggend geval, terwijl aan gelijkaardige gegevenslekken van derden geen gevolg wordt gegeven. Het feit dat het Algemeen Secretariaat volgens haar beoordelingscriteria kennelijk initieel tot het besluit kwam dat er geen opvolging nodig was en dat de melding van het gegevenslek pas maanden later op initiatief van de Inspectiedienst toch werd opgevolgd, toont eveneens aan dat er van

6° te bevelen dat wordt voldaan aan de verzoeken van de betrokkene om zijn rechten uit te oefenen;

7° te bevelen dat de betrokkene in kennis wordt gesteld van het veiligheidsprobleem;

8° te bevelen dat de verwerking tijdelijk of definitief wordt bevroren, beperkt of verboden;

9° te bevelen dat de verwerking in overeenstemming wordt gebracht;

10° de rechtzetting, de beperking of de verwijdering van gegevens en de kennisgeving ervan aan de ontvangers van de gegevens te bevelen;

11° de intrekking van de erkenning van certificatie-instellingen te bevelen;

12° dwangsommen op te leggen;

13° administratieve geldboeten op te leggen;

14° de opschorting van grensoverschrijdende gegevensstromen naar een andere Staat of een internationale instelling te bevelen;

15° het dossier over te dragen aan het parket van de procureur des Konings te Brussel, die het in kennis stelt van het gevolg dat aan het dossier wordt gegeven.

² Arrest van het Marktenhof d.d. 2 september 2020, 9.4.

³ I. OPDEBEEK en S. DE SOMER, « Hoofdstuk III - Beginselen van behoorlijk bestuur » in S. DE SOMER en I. OPDEBEEK (ed.), Algemeen bestuursrecht (tweede editie) - gebonden editie, 2e editie, Brussel, Intersentia, 2019, p. 412-413.

⁴ I. OPDEBEEK en S. DE SOMER, « Hoofdstuk III - Beginselen van behoorlijk bestuur » in S. DE SOMER en I. OPDEBEEK (ed.), Algemeen bestuursrecht (tweede editie) - gebonden editie, 2e editie, Brussel, Intersentia, 2019, p. 412-413.

een gelijke behandeling van gelijke feitenconstellaties in onderhavig geval geen sprake kan zijn.

20. De Geschillenkamer wijst er vooreerst op dat overeenkomstig artikel 72 WOG de inspecteur-generaal en de inspecteurs mogen *“overgaan tot elk onderzoek, elke controle en elk verhoor, alsook alle inlichtingen inwinnen die zij nodig achten om zich ervan te vergewissen dat de grondbeginselen van de bescherming van de persoonsgegevens, in het kader van deze wet en van de wetten die bepalingen bevatten inzake de bescherming van de verwerking van persoonsgegevens, waarop zij toezicht uitoefenen, werkelijk worden nageleefd”*.
21. Gelet op het bovenstaande komt het aan de Inspectiedienst toe om, binnen de hem toegewezen bevoegdheden, alle door haar noodzakelijk geachte onderzoekshandelingen te verrichten. De Geschillenkamer zelf als administratief geschillenorgaan dient haar beslissingen te stoelen op onderzoeksdaden die kennelijk ressorteren binnen het wettelijk kader waarin administratieve bestuursorganen dienen te handelen.⁵ Er is in deze zaak geen enkele aanleiding om de rechtmatigheid van de onderzoekshandelingen van de Inspectiedienst in vraag te stellen.

II.2. Artikel 5, lid 1, a), c) en f) en lid 2, artikel 6, lid 1, artikel 24, lid 1 en artikel 25, lid 1 en lid 2

22. Als verwerkingsverantwoordelijke is de verweerster verplicht de gegevensbeschermingsbeginselen in acht te nemen en moet zij kunnen aantonen dat deze beginselen worden nageleefd (verantwoordingsplicht - artikel 5, lid 2 AVG).
23. Bovendien moet zij, eveneens in haar hoedanigheid van verwerkingsverantwoordelijke, alle nodige maatregelen treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd (artikel 24 en 25 AVG).
24. De Geschillenkamer herinnert eraan dat het uitgangspunt van artikel 5, lid 1, a) AVG is dat persoonsgegevens alleen op rechtmatige wijze mogen worden verwerkt. Dit betekent dat een rechtsgrond voor de verwerking van persoonsgegevens als bedoeld in artikel 6, lid 1 van de AVG aanwezig moet zijn. In verdere uitwerking van dit basisprincipe stelt artikel 6, lid 1 AVG dat persoonsgegevens enkel mogen worden verwerkt op grond van één van de in het artikel opgesomde rechtsgronden. Wanneer persoonsgegevens worden verwerkt dan

⁵ naar analogie met het arrest van het hof van beroep te Brussel (Marktenhof) dd. 7 juli 2021, p. 18: “In het kader van discretionaire bevoegdheden kan de rechter door middel van de beginselen van behoorlijk bestuur nagaan of het bestuur de haar toegemeten bevoegdheid binnen de grenzen van de rechtmatigheid heeft uitgeoefend. Hierbij beschikt de rechter slechts over een marginaal toetsingsrecht. De rechter mag het aangeklaagde gedrag slechts als foutief bestempelen wanneer dit ingaat tegen de opvattingen van elk normaal voorzichtig en redelijk bestuurlijk orgaan. Dit is onder meer het geval wanneer de beslissing niet op concrete gegevens zou berusten en in zou gaan tegen de redelijkheid, en het bestuur bijgevolg een kennelijke beoordelingsfout zou begaan. Het redelijkheidsbeginsel beperkt te discretionaire bevoegdheid enkel doordat het niet duldt dat hetgeen beslist is in kennelijke wanverhouding staat tot de feiten (daarin begrepen alle dossierstukken) waarop de beslissing is gebaseerd.

moeten zij voor het doel toereikend en ter zake dienend zijn. Verder mogen er niet meer persoonsgegevens worden verwerkt dan noodzakelijk voor het doel (artikel 5.1, c) AVG). Artikel 5, 1, f) van de AVG schrijft voor dat “[persoonsgegevens] 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”.

25. Met betrekking tot de litigieuze verwerking stelt de Inspectiedienst in zijn verslag vast dat de verweerster in het kader van de klacht in dit dossier een inbreuk heeft begaan op artikel 5, lid 1, a), c), f) en lid 2 van de AVG op basis van onderstaande elementen :
- het beginsel inzake rechtmatigheid werd geschonden omdat de verzending van persoonsgegevens van de klaagster naar een verkeerde bestemming niet was gebaseerd op een rechtsgrond uit artikel 6, lid 1 van de AVG;
 - het beginsel inzake minimale gegevensverwerking werd geschonden omdat de verweerder meer persoonsgegevens van de klaagster heeft verwerkt dan noodzakelijk was door de verzending ervan naar een verkeerde bestemming;
 - het beginsel inzake integriteit en vertrouwelijkheid werd geschonden omdat de verweerder door de verzending van persoonsgegevens van de klaagster naar een verkeerde bestemming de vertrouwelijkheid van die persoonsgegevens heeft in het gedrang gebracht; en
 - door de verzending van persoonsgegevens van de klaagster naar een verkeerde bestemming heeft de verweerster niet de nodige technische en organisatorische maatregelen genomen om te waarborgen en te kunnen aantonen dat de verwerking heeft plaatsgevonden conform de AVG.
26. Ondanks deze inbreuk op bovenvermelde artikelen in het kader van dit dossier, stelt de Inspectiedienst vast dat de verweerster in het algemeen de verplichtingen opgelegd door artikel 5 van de AVG probeert na te leven. De Inspectiedienst merkt echter op dat dit geen afbreuk doet aan de hierboven vermelde concrete inbreuk.
27. De verweerster erkent dat de e-mail dd. 2 juni 2021 gericht was aan de klaagster, maar dat door een gevolg van een eenmalige menselijke vergissing, onbedoeld de persoonsgegevens betreffende de klaagster aan een derde werden verstuurd. Zij licht toe dat dit het gevolg is van het feit dat het e-mailadres van de raadsman van de klaagster gelijkaardig is aan een ander e-mailadres in het mailsysteem van de verweerster. De verweerster stelt dat dergelijke onbedoelde, niet intentionele handeling, geen aanleiding kan geven tot een inbreuk op de AVG.

28. De verweerster voert aan dat zij alle passende maatregelen genomen heeft om haar verplichtingen inzake gegevensbescherming na te komen en zoveel als mogelijk in te perken. Zo heeft zij de volgende maatregelen genomen die in onderhavige zaak relevant zijn:
- a. Opstellen en uitrollen van een beleid inzake privacy en gegevensbescherming doorheen de onderneming ('Group Compliance Rule Data Protection') die de AVG-vereisten en de invulling ervan voor de entiteiten binnen de Y-groep verduidelijkt;
 - b. Classificatiesysteem van interne en externe e-mails (in categorieën van public, internal, confidential en strictly confidential);
 - c. Implementatie van een waarschuwingsbericht in het e-mailsysteem van de verweerster wanneer medewerkers een e-mail naar een extern e-mailadres sturen;
 - d. Encryptie en wachtwoordbeveiliging van bijlagen bij externe e-mails met (strikt) vertrouwelijke inhoud;
 - e. Maatregelen inzake toegangscontrole tot de systemen van de verweerster;
 - f. Maatregelen inzake afscherming van informatie in de interne systemen van de verweerster;
 - g. Om de departementen proactief te informeren over de zaken waarmee zij rekening moeten houden, werd een "Compliance Checklist" uitgerold met een uitdrukkelijk onderdeel voor Data Protection;
 - h. Opstellen en implementatie van een 'Health Data Framework', dat het beleid en de strategie van de verweerster inzake het verwerken van gezondheidsgegevens omvat. Dit Health Data Framework wordt jaarlijks gereviseerd door vertegenwoordigers van verschillende (risico)functies (Compliance (waar de DPO deel van uitmaakt), Legal, Risk, CC Privacy, Schadebeleid, medische community, ...). Het Framework voorziet concrete richtlijnen en bepaalt de vereisten voor de verwerking van medische gegevens binnen Y Verzekeringen, waaronder (i) regels met betrekking tot de communicatie van gezondheidsgegevens en het gebruik van veilige communicatiekanalen, zowel intern als extern, (ii) specifieke regels rond de verwerking door derden, externe partijen en (iii) specifieke regels rond het bewaren van gezondheidsgegevens;
 - i. Vanuit het domein Information Security geldt een omvattend kader van groepstandaarden die rechtstreeks of onrechtstreeks regels bevatten inzake Data Protection en Privacy, zoals welke communicatiemiddelen gebruikt mogen worden voor welke soort gegevens;
 - j. Training en bewustmaking: de verweerster zorgt ervoor dat haar medewerkers weten hoe zij op een correcte en veilige wijze met persoonsgegevens moeten

omgaan. Alle medewerkers dienen een verplichte basistraining over AVG te volgen. Daarnaast heeft de verweerster een e-learning gelanceerd voor al haar medewerkers die met gezondheidsgegevens omgaan. Deze e-learning focust meer in detail op het verwerken van gezondheidsgegevens en neemt belangrijke delen op zoals onder andere duidelijke richtlijnen inzake het gebruik van beveiligde communicatiekanalen. Een update van deze training werd uitgevoerd en de nieuwe versie werd geïmplementeerd op 24 januari 2022. De trainingen moeten verplicht op geregelde tijdstippen opnieuw gebeuren. De deelname aan deze trainingen wordt geregistreerd en opgevolgd en de opgedane kennis wordt achteraf getoetst door een verplichte test;

- k. Naast de verplichte trainingen, worden er maandelijks berichten gepost over diverse AVG-onderwerpen via het interne communicatieplatform “Y Connect”;
 - l. Naast de interne governance procedures zijn er binnen de verweerster verschillende ondersteunende diensten op dagelijkse basis bezig met adviesverlening en ondersteuning omtrent AVG, met name: (i) het centrale Competence Center Privacy (hierna “CC Privacy”) in eerste lijn, (ii) ondersteund door de Compliance Risk Managers (CORMs) die decentraal zijn aangesteld in eerste lijn en (iii) de Group Compliance Data Protection Unit, waar de DPO van Y Verzekeringen deel van uitmaakt, in de tweede lijn.
29. De verweerster voert aan dat zij verkiest om via veiligere kanalen dan mails te communiceren (zoals bepaalde apps), maar dit is niet altijd mogelijk. Deze zaak betreft communicatie met de raadsman van een klant waardoor e-mail het enige elektronische communicatiekanaal was waarover de verweerster beschikt. Tot slot benadrukt de verweerster dat zij vele inspanningen geleverd heeft om dergelijke risico's te beperken, maar dat een menselijke vergissing steeds een residueel risico zal blijven.
30. De Geschillenkamer vestigt er de aandacht op dat de al dan niet aanwezigheid van een intentie geen criterium vormt voor de al dan niet aanwezigheid van een verwerking van persoonsgegevens in de zin van artikel 4(2) AVG.⁶ Ongeacht of het de bedoeling was van de verweerster om de e-mail te verzenden aan de derde, is het enkele feit dat de e-mail wel degelijk werd verzonden aan de verkeerde bestemming voldoende om deze verzending als verwerking te bestempelen, waarvan de rechtmatigheid dient te worden nagegaan.

⁶ Artikel 4 AVG: “Voor de toepassing van deze verordening wordt verstaan onder:

[...]

2) „verwerking”: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens”

31. Zoals ook erkend door de verweerster is er *in casu* sprake van een inbreuk in verband met persoonsgegevens. Voor zover als nodig herinnert de Geschillenkamer eraan dat een inbreuk in verband met persoonsgegevens een inbreuk op de beveiliging uitmaakt die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Door het verzenden van de e-mail naar de verkeerde bestemming, kon deze derde deze persoonsgegevens van de klaagster ook raadplegen. Er is dan ook sprake van een inbreuk op de vertrouwelijkheid, i.e. een ongeoorloofde of onbedoelde verstrekking van of toegang tot persoonsgegevens. De betrokken persoonsgegevens waren immers onbedoeld blootgesteld gedurende een (korte) periode aan externe personen waardoor de vertrouwelijkheid in het gedrang is gekomen.
32. De Geschillenkamer is van oordeel dat het geheel van de uiteengezette elementen aantoont dat de verweerster zich op geen enkele rechtsgrond uit artikel 6, lid 1, AVG kan beroepen waaruit de rechtmatigheid blijkt van de litigieuze gegevensverwerking. Bovendien is door de gegevensverwerking de vertrouwelijkheid en de integriteit aangetast, nu derden kennis konden nemen van deze gegevens.
33. Voor zoveel als nodig wijst de Geschillenkamer er ook op dat ingevolge artikel 9 AVG gevoelige gegevens, zoals gezondheidsgegevens (*in casu* bevatte de e-mail het feit dat de betrokkene een ongeval heeft gehad met letsel tot gevolg), in beginsel niet verwerkt mogen worden. Op het verwerken van bijzondere categorieën van persoonsgegevens rust gezien hun gevoelige aard dus een algemeen verwerkingsverbod. Hierop is echter wel een beperkt aantal uitzonderingen geformuleerd in de AVG en deze uitzonderingen zijn van toepassing op alle bijzondere categorieën van persoonsgegevens. Ten overvloede wijst de Geschillenkamer op het feit dat voor de litigieuze gegevensverwerking geen van deze uitzonderingen kon worden gebruikt.
34. Dienaangaande is de Geschillenkamer van oordeel dat gelet op het feit dat de verzending een vergissing betrof, het geenszins de bedoeling was om de e-mail naar de verkeerde bestemming te sturen, en de verweerster niet had voorzien dat deze verzending zou gebeuren. Dit vloeit immers voort uit de aard zelf van een vergissing. Het voorgaande geldt des te meer nu in het voorliggende geval geen technische of organisatorische maatregelen bestaan die het risico op het versturen van een e-mail aan een foutieve bestemming door een menselijke vergissing volledig uitsluiten.
35. Niettegenstaande deze inbreuk in verband met persoonsgegevens een inbreuk op de grondbeginselen van artikel 5, lid 1 en artikel 6, lid 1 AVG uitmaakt, stelt de Geschillenkamer vast dat de verweerster de nodige passende technische en organisatorische maatregelen heeft getroffen om de grondbeginselen uit artikel 5, lid 1 na te leven en dit aan te tonen. Uit

het Inspectieverslag blijkt ook dat de verweerder in het algemeen de verplichtingen opgelegd door artikel 5, 24, lid 1 en 25, lid 1 en 2 AVG naleeft. *In casu* betreft de litigieuze verwerking een menselijke fout, waarvan het risico nooit helemaal onbestaande is.

36. In een niet-uitputtende lijst die verwerkingsverantwoordelijken kunnen treffen om aan de verantwoordingsverplichting te voldoen wordt door de Artikel 29 Werkgroep in zijn Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/569⁷ 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. Uit de stukken blijkt dat de verweerder regelmatig awareness-acties uitvoert, het personeel wordt ook bewust gemaakt van de grondbeginselen en verplichtingen voor de verwerkingsverantwoordelijken die voortvloeien uit de AVG. Op deze manier wordt het residueel risico op dergelijke inbreuken in verband met persoonsgegevens tot een minimum herleid.
37. Bijgevolg is de Geschillenkamer van oordeel dat er sprake is van een inbreuk op de artikelen 5, lid 1, a), c) en f) en lid 2, artikel 6, lid 1, artikel 24, lid 1 en artikel 25, lid 1 en lid 2, maar dat het niet noodzakelijk is om hiervoor een geldboete of een correctionele maatregel op te leggen en dat het passend is om een buitenvervolgung te bevelen. In dit kader verwijst de Geschillenkamer naar het feit dat de verweerder het nodige heeft gedaan om van de verkeerde bestemming de verwijdering van de e-mail te verkrijgen alsmede het feit dat de inbreuk niet het gevolg is van een structureel probleem en er voldoende proactieve maatregelen in voege zijn om de overeenstemming met de AVG te waarborgen.

II.3. Artikel 33 van de AVG en artikel 34 van de AVG

II.3.1. Artikel 33 AVG

38. Wanneer dergelijke inbreuk in verband met persoonsgegevens zich voordoet, legt de AVG de verwerkingsverantwoordelijke op om dit te melden aan de bevoegde nationale toezichthoudende autoriteit en, in bepaalde gevallen, om deze inbreuk mee te delen aan de personen op wiens persoonsgegevens de inbreuk betrekking heeft.
39. Voor wat betreft de melding van de inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit verwijst de Geschillenkamer naar artikel 33 AVG dat bepaalt dat *'[i]ndien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de*

⁷ Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wp250rev.01, Artikel 29 Werkgroep.

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. De Inspectiedienst concludeert in zijn verslag dat de melding van de inbreuk aan de GBA en aan de betrokkenen niet tijdig gebeurd is op basis van de volgende vaststellingen. De inbreuk had plaatsgevonden op 2 juni 2022, de interne melding van de inbreuk in verband met persoonsgegevens door de betrokken medewerker aan de Data Protection Unit van de verweerster vond plaats op 4 juni 2022. De melding van de inbreuk in verband met persoonsgegevens aan de GBA vond plaats op 7 juni 2022. Deze melding vond dus plaats meer dan 72 uren na de ontdekking van de inbreuk in verband met persoonsgegevens waardoor er een schending is van de artikelen 33 AVG, aldus het Inspectieverslag.
41. De verweerster betwist deze vaststelling. Zij stelt dat de melding aan de GBA tijdig gebeurd is. De verweerster werpt op dat uit het verslag niet blijkt dat de Inspectiedienst genoegzaam heeft onderzocht op welk ogenblik het tijdstip van kennisname te situeren valt. In tegenstelling tot het Inspectieverslag, betoogt de verweerster dat het startpunt van deze termijn niet het tijdstip is waarop de inbreuk effectief heeft plaatsgevonden, maar wel op het moment dat de verwerkingsverantwoordelijke op de hoogte is gebracht van een mogelijke inbreuk en nadat zij weldegelijk had vastgesteld dat het over een meldingswaardig incident ging. De Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679⁸ van de Artikel 29 Werkgroep bepalen immers dat *“wanneer precies een verwerkingsverantwoordelijke kan worden geacht ‘kennis’ te hebben gekregen van een bepaalde inbreuk, afhangt van de omstandigheden van de specifieke inbreuk”*.⁹ Een verwerkingsverantwoordelijke is volgens de Artikel 29 Werkgroep op de hoogte *“[n]adat de verwerkingsverantwoordelijke voor het eerst door een persoon, een mediaorganisatie of een andere bron op de hoogte is gebracht van een mogelijke inbreuk, of wanneer hij zelf een veiligheidsincident heeft ontdekt, kan hij een kort onderzoek instellen om vast te stellen of er al dan niet daadwerkelijk een inbreuk heeft plaatsgevonden”*¹⁰. Het kan immers enige tijd duren om vast te stellen of persoonsgegevens daadwerkelijk zijn gecompromitteerd: *“Deze korte periode biedt de verwerkingsverantwoordelijke de gelegenheid een onderzoek in te stellen en bewijsmateriaal en andere relevante gegevens*

⁸ Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wp250rev.01, Artikel 29 Werkgroep, p.11-14.

⁹ Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wp250rev.01, Artikel 29 Werkgroep, p.12.

¹⁰ Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, wp250rev.01, Artikel 29 Werkgroep, p.13.

te verzamelen”, zo stelt de verweerster. Verwijzend naar deze richtsnoeren van de Artikel 29 Werkgroep stelt de verweerster dat het startpunt van de termijn van 72 uur uit artikel 33 AVG *in casu* begint te lopen op het moment waarop de verweerster kennis heeft genomen van het feit dat het incident persoonsgegevens betrof die weldegelijk meldingswaardig waren, nadat al de vereiste informatie omtrent het incident door de betrokken medewerker aan de intern bevoegde dienst (Data Protection Unit) werd meegedeeld (met name op 7 juni 2021 om 15u38) en nadat na een analyse weldegelijk was vastgesteld dat het over een meldingswaardig incident ging.

42. Zoals hierboven is uiteengezet, herinnert de Geschillenkamer eraan dat artikel 33 AVG bepaalt dat de verwerkingsverantwoordelijke in geval van een inbreuk in verband met persoonsgegevens verplicht is om de inbreuk zonder onredelijke vertraging te melden en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft gekregen. Het startpunt van de berekening van de termijn van 72 uur start dus op het moment waarop de verweerster als verwerkingsverantwoordelijke er kennis van genomen heeft.
43. Vervolgens rijst de vraag wanneer een verwerkingsverantwoordelijke kan worden geacht "kennis" te hebben gekregen van een inbreuk.
44. Uit de melding van de inbreuk in verband met persoonsgegevens door de verweerster aan de GBA stelt de Geschillenkamer vast dat een medewerker van de verweerster de betrokken mail naar de foutieve bestemming heeft verstuurd op 2 juni 2021 om 17:16. In het meldingsformulier stelt de functionaris voor gegevensbescherming dat de medewerker deze fout ontdekt heeft naar aanleiding van een automatisch antwoord van de bestemming. Vervolgens stuurde zij de e-mail naar de juiste ontvanger op 2 juni 2021 om 17:24. Beide mails werden als stuk toegevoegd aan het dossier. In de melding van de inbreuk in verband met persoonsgegevens aan de GBA wordt het moment waarop het de verweerster kennis heeft genomen van de inbreuk in verband met persoonsgegevens bepaald op 2 juni 2021 om 17:24.
45. Zoals hierboven uiteengezet stelt de verweerster in haar conclusies dat de termijn van 72 uur pas begon te lopen op het moment dat de Data Protection Unit alle relevante documenten heeft ontvangen van de betrokken medewerker om een analyse te kunnen uitvoeren en nadat zij na die analyse had vastgesteld dat het weldegelijk over een meldingswaardig incident ging. In dit kader verwijst de Geschillenkamer naar de Richtsnoeren 9/2022 inzake de meldingen van inbreuken in verband met persoonsgegevens van de EDPB. De European Data Protection Board (hierna: EDPB)¹¹ stelt dat een verwerkingsverantwoordelijke moet worden geacht "kennis" te hebben gekregen

¹¹ EDPB Guidelines 9/2022 on personal data breach notification under GDPR, dd. 10 oktober 2020, te raadplegen via https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf

wanneer hij een redelijke mate van zekerheid heeft dat zich een veiligheidsincident heeft voorgedaan dat tot de compromittering van persoonsgegevens heeft geleid. Dit dient beoordeeld te worden rekening houdende met de omstandigheden van de specifieke inbreuk. De EDPB haalt in deze richtsnoeren enkele situaties aan ter illustratie van wanneer er een redelijke mate van zekerheid is dat er zich een veiligheidsincident heeft voorgedaan, zoals de volgende: *“[e]en derde stelt een verwerkingsverantwoordelijke ervan in kennis dat hij per ongeluk de persoonsgegevens van een van de klanten van de verwerkingsverantwoordelijke heeft ontvangen en levert het bewijs van de ongeoorloofde verstrekking. Aangezien de verwerkingsverantwoordelijke duidelijke bewijzen van een inbreuk op de vertrouwelijkheid heeft ontvangen, kan er geen twijfel over bestaan dat hij daarvan "kennis" heeft gekregen”*.

46. De Geschillenkamer stelt vast dat het bovenvermeld voorbeeld van de EDPB in onderhavige zaak in grote mate gelijklopend is met de feiten van onderhavige zaak. Aangezien de verkeerde bestemming de advocaat van de klager op de hoogte heeft gebracht van de inbreuk met betrekking tot persoonsgegevens, die op haar beurt de verweerster op de hoogte heeft gebracht, was er dus een redelijke mate van zekerheid dat een dergelijk veiligheidsincident zich heeft voorgedaan. De EDPB erkent de mogelijkheid dat een verwerkingsverantwoordelijke een kort onderzoek kan instellen om vast te stellen of er al dan niet daadwerkelijk een inbreuk heeft plaatsgevonden. Zolang dit onderzoek loopt, kan de verwerkingsverantwoordelijke niet worden geacht "kennis" te hebben gekregen.¹² Ook in de situatie die de verweerster opwerpt in de conclusies was er door de e-mail van de raadsman van de klager (en, ten overvloede, doordat de medewerker deze fout blijkbaar zelf ontdekt heeft naar aanleiding van een automatisch antwoord van de verkeerde bestemming) al snel een redelijke mate van zekerheid dat er zich een inbreuk in verband met persoonsgegevens had voorgedaan, en de verweerster er dus kennis van gekregen had.
47. Zodra de verwerkingsverantwoordelijke op dergelijke wijze "kennis" heeft gekregen van een veiligheidsincident, moet een te melden inbreuk zonder onredelijke vertraging en, indien mogelijk, binnen 72 uur worden gemeld aan de toezichthoudende autoriteit indien het waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Gedurende deze periode dient de verwerkingsverantwoordelijke dit waarschijnlijke risico voor personen te beoordelen om na te gaan of de meldingsplicht effectief geldt en welke actie(s) nodig is (zijn) om de inbreuk aan te pakken.¹³
48. Enkel de korte periode die de verwerkingsverantwoordelijke eventueel nodig had om te kunnen beoordelen of dit incident een gegevenslek uitmaakt, is niet inbegrepen in de termijn

¹² EDPB Guidelines 9/2022 on personal data breach notification under GDPR, dd. 10 oktober 2020 , p. 12.

¹³ EDPB Guidelines 9/2022 on personal data breach notification under GDPR, dd. 10 oktober 2020 , p. 12.

van 72 uur (maar gezien hier dus al snel een redelijke mate van zekerheid was, zou deze periode in casu dus bijzonder kort of quasi onbestaande geweest moeten zijn). Deze periode van 72 uur heeft wel tot doel de verwerkingsverantwoordelijke de tijd te geven om een risicoanalyse te doen en om te beoordelen of een melding aan de GBA dient te gebeuren. In tegenstelling tot wat verweerster aanvoert, is deze periode om deze risicoanalyse te doen weldegelijk inbegrepen in de termijn van 72 uur.

49. Deze inbreuk in verband met persoonsgegevens werd pas vrijdag 4 juni 2021 in de loop van de namiddag door de betrokken medewerker gemeld aan de Data Protection Unit. Nadat de Data Protection Unit op de hoogte werd gebracht, werd een risicoanalyse uitgevoerd en werd besloten om deze inbreuk in verband met persoonsgegevens te melden aan de GBA. Deze melding vond plaats op maandag 7 juni 2021 om 21:17. Zoals ook aangegeven in het intern incidentenregister vond deze melding plaats buiten de termijn van 72 uur na de kennisname van het incident (wat te situeren is op 2 juni 2021). Als verklaring werd opgenomen dat de betrokken medewerker de functionaris voor gegevensbescherming laattijdig op de hoogte heeft gebracht. Naar aanleiding hiervan en op vraag van de Data Protection Unit van de verweerster werd een nieuwe *awareness*-actie hieromtrent ondernomen. Gelet op het bovenstaande concludeert de Geschillenkamer dat de laattijdige melding van het gegevenslek aan de GBA een schending van artikel 33 AVG uitmaakt. Gelet op de genomen maatregelen naar aanleiding van dit gegevenslek concludeert de Geschillenkamer dat een berisping passend is. Gelet op de concrete omstandigheden van onderhavige zaak zou het opleggen van een geldboete of een correctionele maatregel onevenredig zijn.

II.3.2. Artikel 34 AVG

50. Overeenkomstig artikel 34 AVG moet de verwerkingsverantwoordelijke in bepaalde gevallen een inbreuk niet alleen melden aan de toezichthoudende autoriteit, maar moet hij ze ook meedelen aan de getroffen personen. Dit is het geval als het waarschijnlijk is dat een inbreuk resulteert in een hoog risico voor de rechten en vrijheden van natuurlijke personen.
51. De drempel voor het meedelen van een inbreuk aan de betrokkenen ligt dus hoger dan die voor het melden van een inbreuk aan de toezichthoudende autoriteiten, en dus behoeven niet alle inbreuken die wel gemeld moeten worden aan de toezichthoudende autoriteit ook aan de betrokken personen gemeld worden.
52. Op basis van artikel 34 van de AVG moet de verwerkingsverantwoordelijke een inbreuk in verband met persoonsgegevens onverwijld meedelen aan de betrokkene “[w]anneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen”. De Geschillenkamer merkt op dat er geen termijn van 72 uur vooropgesteld is voor wat betreft de melding aan de betrokkenen. Deze

melding dient onverwijld te gebeuren omdat het belangrijkste doel van de mededeling aan personen is om specifieke informatie te verstrekken over de stappen die zij moeten ondernemen om zichzelf te beschermen.¹⁴

53. De verweerster heeft in haar melding van het gegevenslek aan de GBA aangegeven dat de betrokkene geïnformeerd zou worden aangezien het verlies van de controle over de persoonsgegevens van de betrokkene door een verspreiding die meer dan noodzakelijk was een hoog risico voor de rechten en vrijheden van de betrokkene inhoudt. Zoals hierboven reeds uiteengezet heeft de Data Protection Unit alle nodige documentatie van de betrokken medewerker ontvangen op 7 juni 2021 om 15u38. Vervolgens kon de Data Protection Unit analyseren of het gegevenslek een hoog risico inhoudt voor de rechten en vrijheden van de klaagster. De klaagster werd vervolgens van het gegevenslek op de hoogte gebracht op de volgende dag.
54. De Geschillenkamer stelt vast dat het gegevenslek heeft plaatsgevonden op 2 juni 2021 en de klaagster hiervan pas op de hoogte werd gesteld op 8 juni 2021. Dit vloeit voort uit het feit dat de betrokken werknemer de Data Protection Unit niet tijdig heeft geïnformeerd van het gegevenslek waardoor deze niet tijdig een analyse kon maken van de impact ervan op de rechten en vrijheden van de klaagster. Gelet op het bovenstaande, is de Geschillenkamer van mening dat er sprake is van schending van artikel 34 AVG. De Geschillenkamer stelt opnieuw vast dat de verweerster, naar aanleiding van dit gegevenslek awareness-acties ondernomen heeft en dat de Data Protection Unit de dag na ontvangst van de noodzakelijke stukken de noodzakelijke analyse in het kader van artikel 34 uitgevoerd heeft. Bijgevolg concludeert de Geschillenkamer dat een berisping passend is, gelet op de concrete omstandigheden van onderhavige zaak.

II.4. Artikel 38, lid 1 en artikel 39 van de AVG

55. De AVG erkent dat de functionaris voor gegevensbescherming een sleutelfiguur is voor wat betreft de bescherming van persoonsgegevens wiens aanwijzing, positie en taken aan regels onderworpen zijn. Deze regels helpen de verwerkingsverantwoordelijke om te voldoen aan haar verplichtingen onder de AVG, maar helpen ook de functionaris voor gegevensbescherming om zijn taken naar behoren uit te oefenen.
56. Artikel 38, lid 1 AVG schrijft voor dat de verwerkingsverantwoordelijke er zorg voor draagt dat de functionaris voor gegevensbescherming tijdig en naar behoren wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De betrokkenheid van de functionaris voor gegevensbescherming moet ertoe bijdragen dat hij de taken vermeld in artikel 39 van de AVG effectief kan vervullen.

¹⁴ Zie ook overweging 86.

57. De Inspectiedienst kwam na onderzoek tot de vaststelling dat geen inbreuk van artikel 38, lid 1 en artikel 39 AVG kon worden vastgesteld. Op basis van de stukken van het dossier en de conclusies van de verweerder is er volgens de Geschillenkamer geen reden om hieromtrent een afwijkend standpunt in te nemen.

III. Publicatie van de beslissing

58. 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, §2 WOG, een buitenvervolginstelling uit te spreken voor wat betreft de inbreuken op
 - o artikel 5, lid 1, a), c) en f) en lid 2, artikel 6, lid 1, artikel 24, lid 1 en artikel 25, lid 1 en lid 2 van de AVG;
- Op grond van artikel 100, §5 WOG, een berisping te formuleren voor wat betreft de inbreuken op
 - o artikel 33 en 34 AVG.

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

Een dergelijk beroep kan worden aangetekend middels een verzoekschrift op tegenspraak dat de in artikel 1034^{ter} van het Gerechtelijk Wetboek opgesomde vermeldingen dient te bevatten¹⁵. Het verzoekschrift op tegenspraak dient te worden ingediend bij de griffie van het Marktenhof

¹⁵ Het verzoekschrift vermeldt op straffe van nietigheid:

- 1° de dag, de maand en het jaar;
- 2° de naam, voornaam, woonplaats van de verzoeker en, in voorkomend geval, zijn hoedanigheid en zijn rijksregister- of ondernemingsnummer;
- 3° de naam, voornaam, woonplaats en, in voorkomend geval, de hoedanigheid van de persoon die moet worden opgeroepen;
- 4° het voorwerp en de korte samenvatting van de middelen van de vordering;
- 5° de rechter voor wie de vordering aanhangig wordt gemaakt;
- 6° de handtekening van de verzoeker of van zijn advocaat.

overeenkomstig artikel 1034^{quinquies} van het Ger.W.¹⁶, dan wel via het e-Deposit informaticasysteem van Justitie (artikel 32^{ter} van het Ger.W.).

(get). Hielke HIJMANS

Voorzitter van de Geschillenkamer

¹⁶ Het verzoekschrift met zijn bijlage wordt, in zoveel exemplaren als er betrokken partijen zijn, bij aangetekende brief gezonden aan de griffier van het gerecht of ter griffie neergelegd.