Streitsachenkammer

Entscheidung 170/2023 vom 20 Dezember 2023

Aktenzeichen: DOS-2019-04346

Gegenstand: Datenleck im Rahmen eines Treueprogramms

Die Streitsachenkammer der Datenschutzbehörde, bestehend aus dem Vorsitzenden Herrn Hielke HIJMANS und den Mitgliedern Herrn Dirk Van Der Kelen und Herrn Christophe Boeraeve;

Aufgrund der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 *zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG* (Datenschutzgrundverordnung), nachstehend DSGVO genannt;

Aufgrund des Gesetzes vom 3. Dezember 2017 *zur Schaffung der Datenschutzbehörde* (nachstehend DSB);

Aufgrund der Geschäftsordnung, wie sie von der Abgeordnetenkammer am 20. Dezember 2018 genehmigt und am 15. Januar 2019 im *Belgischen Staatsblatt* veröffentlicht wurde;

Aufgrund der Aktenlage;

traf die folgende Entscheidung bezüglich:

Der Beklagten: Y, vertreten durch Rechtsanwalt Cédric Burton und Rechtsanwältin Laura Brodahl, im Folgenden „die Beklagte“.

I. Fakten und Verfahren

A. Untersuchung des Inspektionsdienstes

1. Am 20. Dezember 2019 beschloss der Vorstand der Datenschutzbehörde (im Folgenden „DSB"), den Inspektionsdienst der DSB mit einem Fall auf der Grundlage von Artikel 63, 1° der LCA zu befassen, da es offenbar ernsthafte Hinweise darauf gab, dass die Beklagte ihren Verpflichtungen aus Artikel 32 der DSGVO nicht nachgekommen war. Die Faktoren, die der Vorstand in diesem Zusammenhang berücksichtigte, waren das Ausmaß des Datenlecks (die Zahl der betroffenen Personen belief sich auf 89.429 in 27 EU-Mitgliedstaaten) und die Art der offengelegten Daten, d. h. Kartennummer, Name der betroffenen Person, Geburtsdatum, Geschlecht, Adresse, E-Mail-Adresse, Telefonnummer, Mobiltelefonnummer und eine eindeutige Identifikationsnummer.

2. Nachdem das Generalsekretariat der Datenschutzbehörde das am 19. August 2019 bei der Beklagten aufgetretene Datenleck bearbeitet und die Beschwerden, die von Personen in Deutschland in ihrer Eigenschaft als von dem Datenleck betroffene Personen beim First-Line-Service der Datenschutzbehörde eingereicht wurden, bearbeitet hatte, wurde der Fall vom Vorstand geprüft und gemäß Artikel 63, Ziffer 1 der LCA zur Befassung des Inspektionsdienstes weitergeleitet, und die individuellen Beschwerden von deutschen Bürgern wurden, nachdem sie vom First-Line-Dienst für zulässig erklärt worden waren, gemäß Artikel 96 Absatz 1 der LCA *juncto* Artikel 63, Ziffer 2 der LCA ebenfalls an den Inspektionsdienst weitergeleitet.

3. Der Grund für die oben erwähnte Befassung war ein konkretes Datenleck bei einem Subunternehmer der Beklagten. Dieser Subunternehmer betreibt die Plattform (..) Programms, auf der sich Karteninhaber für ein Treueprogramm anmelden können, das auf Punkten basiert, die sie erhalten, wenn sie mit ihrer Karte Einkäufe tätigen. Über diese Plattform konnten die Karteninhaber auf ihre Daten, einschließlich ihres Punktestands, zugreifen und diese dann für Werbeaktionen von teilnehmenden Händlern verwenden, die ihre Angebote auf der Plattform anzeigten. Der Subunternehmer beauftragte seinerseits wiederum einen Subunternehmer mit dem externen Hosting/der externen Protokollierung.

4. Am 20. Juli 2023 wird die Untersuchung des Inspektionsdienstes abgeschlossen, der Bericht wird der Akte beigefügt und diese wird vom Generalinspektor an den Vorsitzenden der Streitsachenkammer weitergeleitet (Art. 91 Absatz 1 und Absatz 2 der LCA), was zur Befassung der Streitsachenkammer gemäß Art. 92, Ziffer 3 GSD geführt hat. In seinem Bericht war der Inspektionsdienst zu dem Schluss gekommen, dass die große Zahl der von dem Datenleck betroffenen Personen und die Einhaltung der Meldepflicht gegenüber der DSB für sich genommen nicht ausreichten, um auf einen Hinweis auf eine Praxis zu schließen, die zu einer Verletzung der Grundprinzipien des Schutzes personenbezogener

Daten im Sinne von Artikel 63, Ziffer 1 der LCA führen könnte. Ansonsten enthält der Inspektionsbericht keine Feststellungen zu einem Verstoß gegen die DSGVO durch die Beklagte.

B. Verfahren vor der Streitsachenkammer

5. Am 27. September 2023 entscheidet die Streitsachenkammer gemäß Artikel 95, Absatz 1, Ziffer 1 und Artikel 98 der LCA, dass die Akte in der Sache behandelt werden kann. Die Beklagte wird per Einschreiben über die Bestimmungen, wie sie in Artikel 95, Absatz 2 sowie Artikel 98 der LCA aufgeführt sind, informiert. Sie wird nach Artikel 99 der LCA auch über die Frist zur Übermittlung der Schlussfolgerung informiert. Die Frist für den Eingang der Klageerwiderung der Beklagten war ursprünglich auf den 30. Oktober 2023 festgelegt, wurde jedoch auf den 15. November 2023 verlängert.
6. Am 6. Oktober 2023 forderte die Beklagte eine Kopie der Akte an (Art. 95, Absatz 2, Ziffer 3 der LCA), die ihr am 18. Oktober 2023 übermittelt und am 25. Oktober 2023 vervollständigt wurde. Die Beklagte erklärt sich auch damit einverstanden, alle Mitteilungen über den Fall auf elektronischem Wege zu erhalten, wie es in Artikel 98 DSG vorgesehen ist.
7. Am 10. November 2023 werden die Parteien darüber informiert, dass die Anhörung am 1. Dezember 2023 stattfinden wird.
8. Am 15. November 2023 erhält die Streitsachenkammer die Antwortschrift der Beklagten. Neben der Verteidigung in der Sache, die sich hauptsächlich auf den technischen Bericht des Inspektionsdienstes bezieht, greifen diese Schlussfolgerungen auch einige verfahrensrechtliche Verteidigungsmittel auf, die sich auf die Art und Weise beziehen, wie der Inspektionsdienst eingeschaltet wurde und die Untersuchung durchführte.
9. Am 1. Dezember 2023 wird die Beklagte von der Streitsachenkammer angehört. Die Beklagte wird daher angehört und erhält die Möglichkeit, ihre Argumente darzulegen.

Anschließend wird der Fall von der Streitsachenkammer beraten.

10. Am 8. Dezember 2023 wird der Beklagten gemäß Artikel 54 der Geschäftsordnung das Protokoll der Anhörung vorgelegt. Der Beklagten wird somit die Gelegenheit geboten, ihre eventuellen diesbezüglichen Anmerkungen im Anhang des Protokolls hinzufügen zu lassen, ohne dass dies eine Wiedereröffnung der Verhandlung bedeutet.
11. Am 15. Dezember 2023 erhält die Streitsachenkammer einige Bemerkungen zum Protokoll, die sie in ihre Beratung aufnehmen will.

II. Begründung

A. Verfahrensweise

12. Die Beklagte argumentiert, dass eine Untersuchung durch den Vorstand oder den Inspektionsdienst nur dann von sich aus eingeleitet werden kann, wenn es ernsthafte Hinweise auf eine Nichteinhaltung gibt. Nach Ansicht der Beklagten hat keines der beiden Organe das Vorhandensein solcher Indizien festgestellt. Beide hätten daher unrechtmäßig eine Untersuchung in Bezug auf die Verarbeitungstätigkeiten der Beklagten durchgeführt.

13. In diesem Zusammenhang muss die Streitsachenkammer darauf hinweisen, dass in dem Vermerk, den das Generalsekretariat nach der Meldung des Datenlecks durch die Beklagte an den Vorstand gerichtet hat und der als Grundlage für die Entscheidung des Vorstands diente, den Fall an den Inspektionsdienst weiterzuleiten, eindeutig erwähnt wird, dass ausreichende Elemente in dem Vermerk auf eine Praxis hinweisen, die zu einer Verletzung der Grundprinzipien des Schutzes personenbezogener Daten führt (Artikel 63, Ziffer 1 der LCA). Im betreffenden Vermerk wird ausdrücklich auf die große Zahl der von diesem Datenleck betroffenen Personen in 27 EU-Mitgliedstaaten hingewiesen. Der Vermerk weist auch darauf hin, dass die DSB bereits sieben Beschwerden von deutschen Bürgern erhalten hat und dass die Aufsichtsbehörde des deutschen Bundeslandes Hessen selbst etwa dreihundert Beschwerden über dieses Datenleck erhalten hat, die noch an die DSB weitergeleitet werden könnten.

14. Die Streitsachenkammer stellt fest, dass es auf der Grundlage des Vermerks sehr wohl ernsthafte Hinweise gab, die auf eine Praxis hindeuten könnten, die zu Datenschutzverletzungen führt. In diesem Zusammenhang galt es, nicht nur die Auswirkungen des Datenlecks auf die große Zahl der betroffenen Personen zu berücksichtigen, sondern auch die Art der Daten, die potenziell aus Finanzdaten bestanden. Nach Ansicht der Streitsachenkammer stellten diese Indizien zumindest eine ausreichende Rechtfertigung für die Prüfung dar, ob die in dem Vermerk erwähnte Erklärung der Beklagten, dass das Zahlungsnetzwerk von der Plattform, auf der die personenbezogenen Daten der Kunden im Rahmen (..) Programms gesammelt werden, getrennt ist, zutreffend ist.

15. Offensichtlich kann erst nach einer Untersuchung durch den Inspektionsdienst festgestellt werden, dass gegebenenfalls keine Praxis im Sinne von Artikel 63 Ziffer 1 der LCA vorliegt. Diese Feststellung des Inspektionsdienstes beeinträchtigt nicht die Rechtmäßigkeit der Entscheidung des Vorstands, dass auf der Grundlage der zu diesem Zeitpunkt und damit vor der Untersuchung des Inspektionsdienstes verfügbaren Elemente ernsthafte Anhaltspunkte vorlagen, die eine Untersuchung durch den Inspektionsdienst erforderten. Die Streitsachenkammer ist daher der Ansicht, dass der Inspektionsdienst in

Übereinstimmung mit Artikel 63, Ziffer 1 der LCA befasst wurde und seine Untersuchung ordnungsgemäß durchgeführt hat.

16. Die Beklagte argumentiert außerdem, dass die DSB keine Behauptung der Nichteinhaltung formuliert. Die Beklagte bezieht sich dabei auf den Inspektionsbericht, in dem keine Verstöße festgestellt wurden, sowie auf das Schreiben der Streitsachenkammer, in dem die Beklagte aufgefordert wird, zu den von ihr ergriffenen Maßnahmen gemäß Art. 24 ff. der DSGVO Stellung zu nehmen.

17. Die Streitsachenkammer erklärt, dass es nachweislich 2019 zu einem Datenleck gekommen ist, dass sie in ihrer Entscheidung jedoch die zwischenzeitlichen Entwicklungen berücksichtigen möchte, um ein umfassendes Bild der aktuellen Situation zu erhalten und so zu einer ausgewogenen Stellungnahme zu gelangen. Nur vor diesem Hintergrund prüfte die Streitsachenkammer den Fall inhaltlich und forderte im Rahmen dieses Verfahrens die Beklagte auf, die ergriffenen technischen und organisatorischen Maßnahmen zu erläutern.

B. Technische und organisatorische Maßnahmen

18. Nach den von ihr vorgelegten Informationen sperrte die Beklagte, sobald sie von dem Datenleck erfuhr, die Webseite des Programms (..) sofort und entfernte alle Zugriffe auf die auf der Plattform gespeicherten Daten. Die Beklagte bewertete die Auswirkungen des Vorfalls und kam zu dem Schluss, dass er kein erhöhtes Risiko für Personen mit sich brachte. Der Vorfall war auf das Programm beschränkt und wirkte sich in keiner Weise auf das Zahlungsnetzwerk der Beklagten aus. Dennoch informierte die Beklagte aus übertriebener Vorsicht auch die betroffenen Personen am 22. August 2019, damit sie eventuelle Vorsichtsmaßnahmen ergreifen konnten, falls diese notwendig sein sollten.

19. In Bezug auf das Datenleck, das zu dieser Entscheidung führte, muss die Streitsachenkammer daher feststellen, dass die Beklagte dieses Datenleck der DSB in dem von Art. 33 DSGVO vorgeschriebenen Rahmen meldete, obwohl das Datenleck von der Beklagten als wenig riskant für die betroffenen Personen bewertet wurde. Was konkret die Meldung des Datenlecks an die DSB betrifft, so handelte die Beklagte im Einklang mit der DSGVO.

20. Darüber hinaus zeigen die Fakten in der Akte, dass es keine wiederholten Datenlecks gab, die auf ein systematisches Versagen der Beklagten hindeuteten, in dessen Folge sie ihren Verpflichtungen nach Art. 24 *juncto* Art. 32 DSGVO nicht nachgekommen wäre. Das Datenleck stellt vielmehr einen völlig isolierten Umstand dar.

21. Darüber hinaus ermöglichten die von der Beklagten in die Akte eingereichten Dokumente der Streitsachenkammer ein tiefgreifendes Verständnis des vorausschauenden Ansatzes der Beklagten, um eine Wiederholung der Ereignisse, wie sie sich ereignet haben, zu

vermeiden. Diese Maßnahmen wurden von der Streitsachenkammer bewertet, die zu folgenden Ergebnissen kam.

22. Die Beklagte entwickelt ihre Verfahren gegenüber den Anbietern weiterhin erfolgreich. Diese Entwicklungen umfassen eine Reihe von Initiativen, die über die gesetzlichen Anforderungen hinausgehen. Im Zusammenhang mit ihrer Verpflichtung zur Gewährleistung einer kontinuierlichen Sicherheit überprüft und verbessert die Beklagte ihre Datensicherheitsmaßnahmen unter Berücksichtigung der auf dem Markt verfügbaren technologischen Fortschritte und folgt dem „Stand der Technik", der sich ständig weiterentwickelt. Insbesondere verfuhr die Beklagte wie folgt:

- Sie aktualisierte ihre Fragebögen zur Sorgfaltspflicht gegenüber Anbietern sowie ihre Richtlinien und Prozesse zur Risikobewertung von Anbietern;
- Sie führte Audits bei aktiven Anbietern in Europa durch;
- Sie führte eine Überprüfung der Zertifizierungen von in Europa tätigen Anbietern durch;
- Sie führte Schulungen für Mitarbeiter verschiedener Abteilungen über die Rollen und Verantwortlichkeiten beim Risikomanagement von Anbietern durch;
- Sie integrierte das Programm für das Anbietermanagement sofort in die anderen Prozesse des Unternehmens;
- Sie fügte ihrem Risikobewertungsmodell eine neue Risikostufe hinzu;
- Sie aktualisierte ihre Tracking-Tools, um diese Kontrolle und das Tracking von Anbietern effizienter zu gestalten und die Tools flexibler zu verwalten;
- Sie erweiterte das Team, das sich mit der Bewertung von Anbietern befasst;
- Sie aktualisierte ihren Fragebogen zur Neubewertung;
- Sie führte eine neue standardisierte Liste von Sicherheitsmaßnahmen ein, an die sich alle Anbieter halten müssen;
- Sie verfeinerte ihren Risikobewertungsprozess, um die Ressourcen effizienter auf die Abteilungen zu verteilen; und
- Sie sorgt für eine ständige Sensibilisierung der Anbieter für das Programm, u. a. durch die Schulung von Führungskräften und die Einbeziehung der obersten Managementebene; und durch die breite Weitergabe der E-Mail-Adresse an die *Business Owners*, damit diese das Team problemlos kontaktieren können, um Hilfe zu erhalten oder wenn sie Probleme mit Anbietern haben.

23. Aus all diesen Elementen ergibt sich, dass (i) die Beklagte nach dem Auftreten des Datenlecks schnell die erforderlichen Maßnahmen ergriffen hat; (ii) der Inspektionsdienst keine Feststellungen getroffen hat, die darauf hindeuten, dass die Beklagte eine

Verletzung begangen hat; (iii) die Beklagte ausführlich dargelegt hat, dass umfassende Maßnahmen ergriffen wurden und dass diese Maßnahmen einer ständigen Aktualisierung unterliegen, um derartige Vorfälle in der Zukunft zu verhindern. Dies veranlasst die Streitsachenkammer zu dem Schluss, dass die Beklagte **keinen Verstoß** gegen die DSGVO begangen hat.

III. Veröffentlichung der Entscheidung

24. Angesichts der Bedeutung der Transparenz in Bezug auf den Entscheidungsprozess der Streitsachenkammer wird diese Entscheidung auf der Website der Datenschutzbehörde veröffentlicht. Gemäß ihrer *Politik bezüglich der Veröffentlichung ihrer Entscheidungen*[1] veröffentlicht die Streitsachenkammer jede ihrer Entscheidungen mit dem Ziel der administrativen Transparenz. Diese Transparenz ist sowohl aufgrund ihrer Aufgaben als Datenschutzkontrollbehörde (Artikel 57.1. b) und d) in Verbindung mit Artikel 51 der DSGVO) als auch aufgrund ihrer Eigenschaft als Verwaltungsbehörde, die den Grundsätzen einer guten Verwaltung unterliegt, erforderlich. In dieser Funktion wird die vorliegende Entscheidung veröffentlicht.

25. Für diesen Zweck ist es jedoch nicht erforderlich, dass die Identifikationsdaten der Parteien direkt mitgeteilt werden.

26. Darüber hinaus wurde bei der Entscheidung über die Veröffentlichung auch berücksichtigt, dass sieben Beschwerden von deutschen Bürgern eingereicht worden waren, die wissen wollten, welche Sicherheitsmaßnahmen die Beklagte ergriffen hatte, um Datenlecks zu verhindern. Diese Beschwerden stehen in direktem Zusammenhang mit dem Datenleck, das Gegenstand dieser Entscheidung ist. Diese Beschwerdeführer haben nicht nur Anspruch auf eine Entscheidung der Streitsachenkammer, die notwendigerweise dieselben Erwägungen wie in der vorliegenden Entscheidung aufgreifen muss, sondern es kann darüber hinaus nicht ignoriert werden, dass die Beschwerdeführer aufgrund der Art der Tatsachen, die ihrer Beschwerde zugrunde liegen und die sich in der vorliegenden Entscheidung gegen die Beklagte richten, Kenntnis von der Identität der Beklagten haben. Die Streitsachenkammer ist jedoch nicht befugt, diesen Beschwerdeführern zu verbieten, die von der Streitsachenkammer getroffene Entscheidung bekannt zu machen oder deren Veröffentlichung zu untersagen. Daher ist die Streitsachenkammer der Ansicht, dass es nicht möglich ist, dem Antrag der Beklagten auf Unterlassung der Veröffentlichung stattzugeben, da die Veröffentlichung der vorliegenden Entscheidung die Beklagte potenziell in ihrem täglichen Betrieb durch eine Flut von Anfragen von Kunden, die zu Unrecht alarmiert wurden, beeinträchtigen könnte.

27. Die Streitsachenkammer ist jedoch der Ansicht, dass die vorliegende Entscheidung im Gegensatz dazu zeigt, dass die Beklagte alles getan hat, um die Verarbeitung der personenbezogenen Daten der Kunden in Übereinstimmung mit der DSGVO durchzuführen, insbesondere im Hinblick auf die Datensicherheit, und ein Beispiel für ihre Branche in Bezug auf den Datenschutz sowie die Aufmerksamkeit und die kontinuierlichen

[1] Datenschutzbehörde, Streitsachenkammer, Veröffentlichungspolitik für Entscheidungen der Streitsachenkammer vom 23. Dezember 2020: https://www.autoriteprotectiondonnees.be/publications/politique-de-publication-des-decisions-de-la-chambre-contentieuse.pdf

Maßnahmen darstellt, die ergriffen wurden, um sich ständig an die Entwicklungen in diesem Bereich anzupassen.

AUS DIESEN GRÜNDEN,

beschließt die Streitsachenkammer der Datenschutzbehörde nach Beratung, die vorliegende Beschwerde gemäß Artikel 100, Absatz 1, Ziffer 1 der LCA ohne weitere Maßnahmen einzustellen, da in dieser Hinsicht kein Verstoß gegen die DSGVO festgestellt werden kann.

Gemäß Artikel 108, Absatz 1 der LCA kann gegen diese Entscheidung innerhalb von 30 Tagen nach ihrer Bekanntgabe Beschwerde beim Märktegerichtshof (Berufungsgericht Brüssel) eingelegt werden, wobei die Datenschutzbehörde (DSB) als Beklagte auftritt.

Ein solcher Rechtsbehelf kann mittels eines Zwischenantrags eingereicht werden, der die in Artikel 1034*ter* des Gerichtsgesetzbuches aufgeführten Informationen enthalten muss[2]. Der Zwischenantrag muss gemäß Artikel 1034*quinquies* des belgischen Gerichtsgesetzbuchs[3] bei der Geschäftsstelle des Märktegerichtshofs eingereicht werden oder über das Informationssystem e-Deposit des Justizministeriums (Artikel 32*ter* des belgischen Gerichtsgesetzbuchs).

(get). Hielke HIJMANS

Vorsitzender der Streitsachenkammer

[2] Der Antrag enthält, unter Androhung der Nichtigkeit, die folgenden Angaben:

1° die Angabe von Tag, Monat und Jahr;
2° Name, Vorname, Anschrift des Antragstellers, sowie gegebenenfalls seine Eigenschaften und seine Nationalregisternummer oder Unternehmensnummer;
3° Name, Vorname, Anschrift und, falls zutreffend, die Eigenschaft der Person, die vorgeladen werden soll;
4° den Gegenstand und eine kurze Darstellung der Gründe für den Antrag;
5° die Angabe des Richters, der mit dem Antrag befasst ist;
6° die Unterschrift des Antragstellers oder seines Anwalts.

[3] Der Antrag und seine Anlage werden in so vielen Ausfertigungen wie Parteien beteiligt sind per Einschreiben an den Gerichtsschreiber des Gerichts gesandt oder bei der Kanzlei hinterlegt.