BVGer A-3790/2024 vom 8. April 2026

Bundesverwaltungsgericht, 2026-04-08, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/bvger_A-3790_2024

FR: TAF A-3790/2024 du 8 avril 2026

IT: TAF A-3790/2024 del 8 aprile 2026

Regeste

Datenschutz

Erwägungen

E. 1.1

Das Bundesverwaltungsgericht beurteilt gemäss Art. 31 VGG Beschwerden gegen Verfügungen nach Art. 5 VwVG, sofern - wie im vorliegenden Fall - keine Ausnahme nach Art. 32 VGG vorliegt. Als Vorinstanzen gelten gestützt auf Art. 33 Bst. d VGG unter anderem die der Bundeskanzlei administrativ zugeordneten Dienststellen der Bundesverwaltung. Die Vereinigte Bundesversammlung wählt die Leiterin oder den Leiter des EDÖB (die oder der Beauftragte; Art. 43 des Datenschutzgesetzes vom 25. September 2020 [DSG, SR 235.1]). Art. 43 Abs. 4 DSG ordnet den EDÖB administrativ der Bundeskanzlei zu; Anhang 1 Bst. A Ziff. 2.1.1 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998 (RVOV, SR 172.010.1) erklärt den EDÖB zur Verwaltungseinheit der dezentralen Bundesverwaltung; dieser gilt daher als Vorinstanz des Bundesverwaltungsgerichts. Die angefochtene Verfügung stellt zudem ein taugliches Anfechtungsobjekt dar. Das Bundesverwaltungsgericht ist somit zur Beurteilung der vorliegenden Beschwerde zuständig. Das Verfahren richtet sich nach dem VwVG, soweit das VGG nichts anderes bestimmt (Art. 37 VGG).

E. 1.2

Die Beschwerdeführerin hat sich am vorinstanzlichen Verfahren beteiligt und ist als Adressatin der angefochtenen Verfügung sowohl formell als auch materiell beschwert, weshalb sie zur Beschwerde legitimiert ist (vgl. Art. 48 Abs. 1 VwVG).

E. 1.3

Auf die im Übrigen frist- und formgerecht eingereichte Beschwerde (Art. 50 Abs. 1 und Art. 52 Abs. 1 VwVG) ist somit einzutreten.

E. 2

Das Bundesverwaltungsgericht entscheidet grundsätzlich mit uneingeschränkter Kognition; es überprüft die angefochtene Verfügung auf Rechtsverletzungen - einschliesslich der unrichtigen und unvollständigen Feststellung des rechtserheblichen Sachverhalts und von Rechtsfehlern bei der Ausübung des Ermessens - sowie auf Angemessenheit hin (Art. 49 VwVG). Das Bundesverwaltungsgericht stellt sodann den rechtserheblichen Sachverhalt unter Vorbehalt der Mitwirkungspflichten der Parteien von Amtes wegen fest (Art. 12 und Art. 13 VwVG) und wendet das Recht grundsätzlich frei und von Amtes wegen an, ohne an die rechtliche Begründung der Parteibegehren gebunden zu sein (Art. 62 Abs. 4 VwVG).

E. 3

Die Beschwerdeführerin rügt die Verletzung des Anspruchs auf rechtliches Gehör in mehrfacher Hinsicht. Vorab ist daher auf die rechtlichen Grundlagen dieses Anspruchs einzugehen.

E. 3.1.1

Gemäss Art. 29 Abs. 2 BV haben die Parteien Anspruch auf Gewährung des rechtlichen Gehörs. Das rechtliche Gehör dient einerseits der Sachaufklärung, anderseits stellt es ein persönlichkeitsbezogenes Mitwirkungsrecht beim Erlass eines Entscheides dar, der in die Rechtsstellung des Einzelnen eingreift. Dazu gehört insbesondere das Recht des Betroffenen, sich vor Erlass eines solchen Entscheids zur Sache zu äussern, erhebliche Beweise beizubringen und Einsicht in die Akten zu nehmen (BGE 140 I 99 E. 3.4; 135 II 286 E. 5.1). Voraussetzung des Äusserungsrechts sind genügende Kenntnisse über den Verfahrensverlauf, was auf das Recht hinausläuft, in geeigneter Weise über die entscheidwesentlichen Vorgänge und Grundlagen vorweg orientiert zu werden (BGE 141 I 60 E. 3.3; 140 I 99 E. 3.4; Urteil des Bundesgerichts [BGer] 2C_50/2024 vom 23. Januar 2025 E. 4.1.1 mit weiteren Hinweisen). Wie weit dieses Recht geht, lässt sich nicht generell, sondern nur unter Würdigung der konkreten Umstände beurteilen (BGE 135 I 279 E. 2.3; 111 Ia 273 E. 2b). Entscheidend ist, ob der betroffenen Person ermöglicht wurde, ihren Standpunkt wirksam zur Geltung zu bringen (BGE 144 I 11 E. 5.3 mit weiteren Hinweisen; Urteil des BGer 2C_807/2015 vom 18. Oktober 2016 E. 2.2.1).

E. 3.1.2

Aus dem Anspruch auf rechtliches Gehör leitet sich zudem die allgemeine Aktenführungspflicht der Behörden ab. Sie ist das Gegenstück zum Akteneinsichts- und Beweisführungsrecht der Parteien (BGE 142 I 86 E. 2.2; Urteil des BGer 2C_143/2023 vom 18. März 2025 E. 3.2.3). Aufgrund dieser Aktenführungspflicht haben die Behörden alles in den Akten festzuhalten, was zur Sache gehört und entscheidwesentlich sein kann (Urteil des BGer 1C_285/2022 vom 25. Juni 2024 E. 5.1; BGE 130 II 473 E. 4.1).

E. 3.1.3

Aus dem Anspruch auf rechtliches Gehör folgt weiter, dass die Behörde die Vorbringen des vom Entscheid in seiner Rechtsstellung Betroffenen auch tatsächlich hört (Art. 31 VwVG), prüft und in der Entscheidfindung berücksichtigt. Art. 32 VwVG, wonach die Behörde alle erheblichen und rechtzeitigen Vorbringen der Parteien würdigt, bevor sie verfügt, hängt eng mit dem Begründungserfordernis (Art. 35 Abs. 1 VwVG) zusammen. Ob sich die Behörde nämlich tatsächlich mit allen erheblichen Vorbringen der Parteien befasst und auseinandergesetzt hat, lässt sich erst aufgrund der Begründung erkennen. Ein Teilaspekt des Anspruchs auf rechtliches Gehör (Art. 29 Abs. 2 BV) ist die Pflicht der Gerichtsbehörde, ihren Entscheid gehörig zu begründen. Die Begründung einer Verfügung hat im Allgemeinen den rechtserheblichen Sachverhalt sowie die anwendbaren Rechtsnormen zu enthalten und sodann die rechtliche Würdigung des Sachverhalts unter die Rechtsnormen (Subsumtion) aufzuzeigen. In diesem Sinne sind wenigstens kurz die Überlegungen zu nennen, von denen sich die Behörde bei ihrem Entscheid hat leiten lassen und auf die sich ihr Entscheid stützt (Urteil des BGer 1C_390/2024 vom 21. Februar 2025 E. 3.1 mit weiteren Hinweisen; Urteil des BVGer A-3149/2024 vom 17. September 2025 E. 3.1 mit weiteren Hinweisen). Bei der Begründung ist es nicht erforderlich, dass sie sich mit allen Parteistandpunkten einlässlich auseinandersetzt und jedes einzelne Vorbringen ausdrücklich widerlegt. Vielmehr kann sie sich auf die für den Entscheid wesentlichen

Punkte beschränken. Die Begründung muss so abgefasst sein, dass der Betroffene sich über die Tragweite des Entscheids ein Bild machen und ihn sachgerecht anfechten kann (BGE 144 I 11 E. 5.3; Urteil des BGer 1C_70/2021 vom 7. Januar 2022 E. 2.1).

E. 3.2.1

Die Beschwerdeführerin macht geltend, die Vorinstanz habe ihr das rechtliche Gehör mit Schreiben vom 29. April 2024 - gleichzeitig mit der Eröffnung der Untersuchung - gewährt, indem sie ihr eine Frist angesetzt habe, um den Entwurf der Sachverhaltsdarstellung zu prüfen und allfällige Korrekturen mitzuteilen. Mit Schreiben vom 12. Mai 2024 habe sie sodann Stellung genommen. Dieses Schreiben habe die Vorinstanz in der angefochtenen Verfügung weder erwähnt noch über die damit verbundenen Anträge zu den Korrekturen entschieden. Der Sachverhalt der angefochtenen Verfügung ende denn auch mit ihrer E-Mail vom 21. März 2024 an die Vorinstanz und beziehe sich nicht auf das Untersuchungsverfahren. Damit werde unter anderem der Eindruck erweckt, die Vorinstanz habe das rechtliche Gehör nur «pro forma» gewährt.

E. 3.2.2

Die Vorinstanz entgegnet im Wesentlichen, sie habe die von der Beschwerdeführerin mit Schreiben vom 12. Mai 2024 beantragten Korrekturen zum Sachverhalt einzeln geprüft. Soweit diese für den rechtserheblichen Sachverhalt relevant gewesen seien, habe sie die Korrekturen berücksichtigt und in die Ziffern 2.1, 2.7 und 2.8 der angefochtenen Verfügung aufgenommen.

E. 3.2.3

Dass die Vorinstanz der Beschwerdeführerin mit Schreiben vom 29. April 2024 das rechtliche Gehör gewährte und ihr damit die Gelegenheit gab, sich vor Erlass der Verfügung zur Sache zu äussern und ihren Standpunkt geltend zu machen, ist unbestritten. Bestritten ist hingegen, dass die Vorinstanz die Vorbringen der Beschwerdeführerin geprüft und in der Entscheidfindung berücksichtigt hat. Mit Schreiben vom 12. Mai 2024 hat die Beschwerdeführerin von ihrem Recht auf rechtliches Gehör Gebrauch gemacht und ausführlich Stellung genommen. Sie äusserte sich eingehend zum Sachverhalt und beantragte die Anpassung der Ziffern 2.1, 2.3, 2.5, 2.6, 2.7, 2.8 und 2.9 des Entwurfes der Sachverhaltsfeststellung (vgl. dazu die nachstehende E. 4.5). Das Schreiben vom 29. April 2024 der Vorinstanz - mit welchem sie einerseits die Untersuchung gegen die Beschwerdeführerin eröffnete und ihr andererseits das rechtliche Gehör gewährte wurde unter Buchstabe A, Ziffer 2 der angefochtenen Verfügung nicht aufgeführt. Dieses Schreiben befindet sich jedoch in den Akten. Dass die Vorinstanz das Schreiben vom 12. Mai 2024 der Beschwerdeführerin berücksichtigt hat, obwohl es ebenfalls nicht unter Buchstabe A, Ziffer 2 der angefochtenen Verfügung aufgeführt ist, ergibt sich aus dem Umstand, dass sie dieses ebenfalls zu den Akten genommen und in den Ziffern 2.1, 2.7 und 2.8 der angefochtenen Verfügung Änderungen vorgenommen hat. Der (vertretenen) Beschwerdeführerin war es diesbezüglich möglich, sich ein Bild über die Tragweite der behördlichen Beurteilung zu machen und die Verfügung sachgerecht anzufechten. Das rechtliche Gehör wurde entsprechend nicht verletzt. Die Frage, ob die Vorinstanz sämtliche Ausführungen der Beschwerdeführerin zum Sachverhalt in der angefochtenen Verfügung hätte übernehmen müssen, ist nachfolgend im Rahmen der Rüge der unrichtigen respektive unvollständigen Sachverhaltsfeststellung zu beurteilen (vgl. dazu die nachstehenden E. 4.2.1 f.).

E. 3.3.1
Die Beschwerdeführerin rügt ausserdem, die Vorinstanz verweise lediglich pauschal und ohne konkreten Bezug zur vorliegenden Angelegenheit auf das sogenannte Phishing als Gefahr, ohne ihr in dieser Hinsicht das rechtliche Gehör gewährt zu haben.

E. 3.3.2
Die Vorinstanz hat sich zu diesem Vorwurf der Gehörsverletzung nicht vernehmen lassen.

E. 3.3.3
Art. 29 Abs. 2 BV verschafft den Anspruch, in geeigneter Weise über die entscheidwesentlichen Vorgänge und Grundlagen vorweg orientiert zu werden. Dies betrifft in erster Linie den rechtserheblichen Sachverhalt und nur in Ausnahmefällen auch Rechtsnormen oder von den Behörden vorgesehene rechtliche Begründungen. Es gibt insbesondere kein Recht, sich vorweg zu jedem Ergebnis oder Detail des zukünftigen Entscheids äussern zu können oder dessen Begründung vorab zur Stellungnahme zu erhalten (Urteil des BGer 1C_235/2019 vom 24. Januar 2020 E. 2.2).

E. 3.3.4
Der angefochtenen Verfügung ist zu entnehmen, dass die Vorinstanz Phishing im vorliegenden Fall als möglich erachtet. Damit war es für die (vertretene) Beschwerdeführerin auch diesbezüglich möglich, sich ein Bild über die Tragweite der behördlichen Beurteilung zu machen und die Verfügung sachgerecht anzufechten. Die Vorinstanz war vorliegend nicht verpflichtet, der Beschwerdeführerin diese Begründung vorab zur Stellungnahme zuzustellen. Eine Gehörsverletzung liegt damit nicht vor.

E. 3.4.1
Die Beschwerdeführerin rügt sinngemäss weiter, die Vorinstanz verweise einerseits auf die Möglichkeit einer öffentlichen Bekanntmachung gemäss Art. 24 Abs. 5 Bst. c DSG, also auf eine Einschränkung der Informationspflicht der betroffenen Personen nach Art. 24 Abs. 4 DSG. Andererseits führe sie aus, es seien keine Ausnahmen der Informationspflicht gestützt auf Art. 24 Abs. 5 DSG ersichtlich. Sodann sei die Information der von der Datenschutzverletzung betroffenen Personen verfügt worden, obwohl deren Identifikation nicht mehr möglich sei. Aufgrund dessen, dass die Vorinstanz festgehalten habe, es lägen keine Ausnahmegründe von der Informationspflicht der betroffenen Personen nach Art. 24 Abs. 4 DSG vor, müsste sie (die Beschwerdeführerin) diese individuell und direkt informieren - was jedoch nicht möglich sei, da sie nicht mehr identifiziert werden könnten -, um die strafbewehrte Verfügung nicht zu verletzen. Damit macht die Beschwerdeführerin sinngemäss (auch) eine Verletzung der Begründungspflicht geltend.

E. 3.4.2
Die Vorinstanz hat sich zu diesem Vorwurf der Gehörsverletzung nicht vernehmen lassen.

E. 3.4.3
Die Vorinstanz hält in der angefochtenen Verfügung einerseits fest, eine Information der betroffenen Personen sei nicht unmöglich, jedoch unverhältnismässig. Gleichzeitig weist sie darauf hin, dass in der vorliegenden Konstellation Art. 24 Abs. 5 Bst. c DSG respektive die öffentliche Bekanntmachung zur Anwendung gelangen könne. Weitergehende Ausführungen enthält die angefochtene Verfügung nicht. Eine Auseinandersetzung mit der öffentlichen Bekanntmachung fehlt gänzlich. Andererseits führt sie auf, es seien keine

Gründe nachgewiesen worden, die eine Einschränkung der Information der Betroffenen rechtfertigen würden. Im Dispositiv verpflichtet die Vorinstanz die Beschwerdeführerin sodann zur Information der betroffenen Personen, ohne dies zu präzisieren. Indem sie die individuelle Information als unverhältnismässig qualifiziert, gleichzeitig jedoch ohne klare Differenzierung respektive ohne Erklärung die Pflicht zur Information der betroffenen Personen verfügt, ist die angefochtene Verfügung nicht nachvollziehbar und mithin unzureichend begründet. Die Vorinstanz hat folglich den Anspruch der Beschwerdeführerin auf eine nachvollziehbare und schlüssige Begründung der Verfügung in schwerwiegender Weise verletzt.

E. 3.4.4

Der Anspruch auf rechtliches Gehör ist formeller Natur. Eine Gehörsverletzung führt ungeachtet der materiellen Begründetheit des Rechtsmittels zur Gutheissung der Beschwerde und zur Aufhebung des angefochtenen Entscheids (BGE 144 I 11 E. 5.3; 142 II 218 E. 2.8.1). Sie kann ausnahmsweise als geheilt gelten, wenn die Gewährung des rechtlichen Gehörs in einem Rechtsmittelverfahren nachgeholt wird, die Rechtsmittelinstanz mit der gleichen Kognition prüft wie die Vorinstanz, die Gehörsverletzung nicht besonders schwer wiegt und der betroffenen Partei durch Heilung kein Nachteil entsteht (vgl. BVGE 2017 I/4 E. 4.2; 2018 IV/5 E. 13.2; 2019 VII/6 E. 4.4). Unter diesen Voraussetzungen ist darüber hinaus - im Sinne einer Heilung des Mangels - selbst bei einer schwerwiegenden Verletzung des Anspruchs auf rechtliches Gehör von einer Rückweisung der Sache an die Vorinstanz abzusehen, wenn und soweit die Rückweisung zu einem formalistischen Leerlauf und damit zu unnötigen Verzögerungen führen würde, die mit dem Interesse der betroffenen Partei an einer beförderlichen Beurteilung der Sache nicht zu vereinbaren wären (BGE 137 I 195 E. 2.3.2 m.w.H.; BVGE 2019 VII/6 E. 4.4 m.w.H.). Die Verletzung des rechtlichen Gehörs kann im Beschwerdeverfahren vor dem Bundesverwaltungsgericht geheilt werden, da dieses über die gleiche Kognition verfügt wie die Vorinstanz (vgl. E. 2). Zudem hatte die Beschwerdeführerin die Gelegenheit, sich vor dem Bundesverwaltungsgericht umfassend zu äussern, wovon sie Gebrauch gemacht hat. Es ist nicht ersichtlich, inwiefern ihr aus der Heilung ein unzumutbarer Nachteil entstehen sollte. Selbst wenn der genannte Verstoss schwer wiegt, würde eine Rückweisung an die Vorinstanz einzig dazu führen, dass diese - wie im Beschwerdeverfahren - begründet, weshalb eine öffentliche Bekanntmachung angezeigt ist, ohne dass mit einem anderen materiellen Ergebnis zu rechnen wäre. Eine solche Rückweisung würde zu einem formalistischen Leerlauf führen und ist prozessökonomisch nicht angezeigt. Die Verletzung des Anspruchs auf rechtliches Gehör gilt daher im Beschwerdeverfahren als geheilt. Der Verletzung von Art. 29 Abs. 2 BV ist jedoch im Kostenpunkt und bei den Entschädigungsfolgen des vorliegenden Verfahrens Rechnung zu tragen.

E. 4.1

Mit Verfügung vom 28. Mai 2024 verpflichtete die Vorinstanz die Beschwerdeführerin, die von der am 16. Februar 2024 gemeldeten Datensicherheitsverletzung betroffenen Personen innert 10 Tagen ab Rechtskraft der Verfügung zu informieren.

E. 4.2

Die Beschwerdeführerin beantragt die Aufhebung dieser Verfügung vom 28. Mai 2024. Sie begründet dies damit, die Vorinstanz habe den Sachverhalt in verschiedener Hinsicht

sowohl unrichtig als auch unvollständig festgestellt (vgl. nachstehende E. 4.2.1 f.) und Bundesrecht verletzt (vgl. nachstehende E. 6.1).

E. 4.2.1

Die Rüge der unrichtigen Feststellung des rechtserheblichen Sachverhaltes durch die Vorinstanz begründet die Beschwerdeführerin im Wesentlichen damit, der unter Bst. A, Ziffer 2.1 der angefochtenen Verfügung aufgeführte Sachverhalt sei sowohl unvollständig als auch fehlerhaft. Mit der Meldung an die Vorinstanz habe sie dieser mitgeteilt, dass die ursprüngliche Information, die sie von der Drittperson erhalten habe, nicht richtig gewesen sei. Sie selbst habe nämlich feststellen können, dass nur ein kleiner Teil der RMA-URLs im Index der Suchmaschine Bing von Microsoft zu finden gewesen sei. Im Index anderer Suchmaschinen, insbesondere bei Google, seien keine RMA-URLs auffindbar gewesen. Auch sei nicht korrekt, dass die RMA-URLs im Internet öffentlich einsehbar gewesen seien. Richtig sei hingegen, dass die URLs ihrer Kundschaft unter Verwendung der Software von Microsoft an Microsoft beziehungsweise den Index der Suchmaschine Bing von Microsoft übermittelt worden seien. Unbekannt sei, ob die betroffene Kundschaft im Rahmen ihrer Einwilligung der Nutzung von Microsoft-Produkten auch in die Bearbeitung ihrer Daten für die Suchmaschine Bing und deren Index eingewilligt hätten. Denn damit würde jegliche Verletzung der Datensicherheit entfallen. Die Beschwerdeführerin führt zusammengefasst weiter aus, die RMA-URLs seien nur den betreffenden einzelnen Kundinnen und Kunden bekannt. Sie gehe entsprechend davon aus, dass der betroffene Teil der Kundschaft die RMA-URLs, vermutlich ohne Absicht durch Bing habe indexieren lassen. Entsprechend seien die einzelnen Supportfälle ausschliesslich für bestimmte Kundinnen und Kunden im Internet einsehbar gewesen. Auch darauf habe sie die Vorinstanz mit Schreiben vom 12. Mai 2024 hingewiesen.

E. 4.2.2

Die Rüge der unvollständigen Feststellung des rechtserheblichen Sachverhaltes durch die Vorinstanz begründet die Beschwerdeführerin im Weiteren auch damit, dass die Vorinstanz unter Bst. B, Ziffer II.1.19 in der angefochtenen Verfügung festhalte, dass die Risikoeinschätzung, die zur Meldung geführt habe, von ihr weder in der Folgemeldung noch in der Stellungnahme vom 21. März 2024 angepasst worden sei. Dies sei zwar korrekt, aber unvollständig. Mit Schreiben vom 12. Mai 2024 habe sie die Vorinstanz ausdrücklich darauf hingewiesen, dass es zum damaligen Zeitpunkt keine Anzeichen gegeben habe, dass sich die möglichen Folgen für die betroffene Kundschaft tatsächlich manifestiert hätten. Sie habe beispielsweise keine Kenntnis von Gutscheinen, die durch Drittpersonen über die gezielte Suche im Index der Suchmaschine Bing gefunden und eingelöst worden seien und entsprechend von der eigentlich berechtigten Kundschaft nicht mehr hätten eingelöst werden können. Es sei nämlich davon auszugehen, dass sich die Kundschaft bei ihr gemeldet hätte, wenn deren Gutscheine nicht mehr hätten eingelöst werden können. Dieser Hinweis bezüglich die Gutscheine betreffe einerseits die möglichen (negativen) Folgen und andererseits die Eintrittswahrscheinlichkeit, wie sie Teil jeder klassischen Risikobeurteilung bilden würden. Vorliegend seien weder die Folgen noch die Eintrittswahrscheinlichkeit (entgegen den anfänglichen Erwartungen) vorhanden gewesen oder zumindest hätten sich diese als tief erwiesen, da keine einzige Rückmeldung von Kundinnen und Kunden erfolgt sei.

E. 4.3

Die Vorinstanz entgegnet im Wesentlichen, sie habe die mit Schreiben vom 12. Mai 2024 vorgebrachten Korrekturwünsche der Beschwerdeführerin soweit nötig übernommen. In der angefochtenen Verfügung sei keine Suchmaschine erwähnt, da diese für den Sachverhalt nicht relevant sei. Entscheidend sei, dass Supportfälle und dadurch potenzielle Personendaten der Kundschaft der Beschwerdeführerin im Internet einsehbar gewesen seien. Mittels welcher Suchmaschine diese Resultate erzielt worden seien, könne nicht entscheidend sein. Ebenso wenig sei die Argumentation haltbar, dass die Kundschaft selbst mittels Einwilligung in die Indexierung durch eine Suchmaschine zugestimmt hätte. Die Beschwerdeführerin habe schliesslich selbst den Zugriff des Suchmaschinen-Crawlers im Nachgang blockiert, eine Massnahme, welche die Kundschaft selbst nicht hätte vornehmen können. Auch würden die Ausführungen zur Auffindbarkeit von URL und RMA-URL ins Leere führen. Der Umstand, dass eine URL durch eine lange und nicht zu erratende Zeichenreihe geschützt gewesen sei, schliesse nicht aus, dass diese dennoch öffentlich einsehbar gewesen sei. Die Datensicherheitsverletzung habe gerade gezeigt, dass der Schutz nicht genügend gewesen sei. Vorliegend seien die Personendaten über mehrere Monate im Internet auffindbar gewesen. Würden die Personen vom Verantwortlichen nicht über eine Datensicherheitsverletzung informiert, hätten sie nicht die Möglichkeit, ihre Aufmerksamkeit gegenüber der möglichen betrügerischen Nutzung ihrer Daten durch Dritte zu erhöhen. Die Ausführungen der Beschwerdeführerin, dass sie keine Meldungen zu tatsächlich entstandenen Schäden der Kundschaft erhalten habe, sei nicht zielführend. Die Information der betroffenen Person nach Art. 24 Abs. 4 DSG habe präventiven Charakter und solle den Schaden verhindern, indem den Betroffenen ermöglicht werde, sich selbst zu schützen, so dass kein Schaden eintrete. Der Nachweis eines konkreten Schadens sei für die Information der betroffenen Person nach Art. 24 DSG keine Voraussetzung.

E. 4.4

Unrichtig ist eine Sachverhaltsfeststellung etwa dann, wenn der Verfügung ein aktenwidriger oder nicht weiter belegbarer Sachverhalt zugrunde gelegt wurde und wenn Beweise unzutreffend gewürdigt wurden. Unvollständig ist die Sachverhaltsfeststellung, wenn die Behörde trotz entsprechender Verpflichtung den rechtserheblichen Sachverhalt nicht von Amtes wegen abgeklärt oder nicht alle für den Entscheid wesentlichen Sachumstände berücksichtigt hat. Die fehlerhafte Sachverhaltsfeststellung muss sich stets auf den wesentlichen, das heisst rechtserheblichen Sachverhalt beziehen und mithin für den Ausgang der Streitigkeit erheblich (sog. entscheidwesentlich) sein (vgl. zum Ganzen Urteil des Bundesverwaltungsgerichts [BVGer] A- 5566/2022 vom 15. Februar 2023 E. 5.2.1).

E. 4.5.1

Die Vorinstanz hält unter Bst. A, Ziffer 2.1 der angefochtenen Verfügung fest, gemäss der Meldung vom 16. Februar 2024 seien «seit Juni 2023 Supportfälle der apfelkiste.ch im Internet einsehbar und von Suchmaschinen indiziert» worden. Der von der Beschwerdeführerin ergänzte Sachverhalt, wonach lediglich ein kleiner Teil der RMA-URLs im Index der Suchmaschine Bing von Microsoft zu finden gewesen sei und die einzelnen Supportfälle ausschliesslich für bestimmte Kundinnen und Kunden im Internet einsehbar gewesen seien, ist in der angefochtenen Verfügung nicht enthalten.

E. 4.5.2

Unter Bst. A, Ziffer 2.3 der angefochtenen Verfügung führt die Vorinstanz auf, die Beschwerdeführerin habe die Datensicherheitsverletzung, so beschrieben, dass der

Kundschaft der apfelkiste.ch für die Meldung von Problemen bei Bestellungen ein Onlineformular zur Verfügung stehe. Die Kundschaft müsse die Bestellnummer und die für die Bestellung verwendete E-Mail-Adresse eingeben, um Meldung erstatten zu können. Für die weitere Kommunikation erhalte die Kundschaft nach ihrer Meldung einen Link mit einem Hashwert an ihre für die Bestellung verwendete E- Mail-Adresse. In der angefochtenen Verfügung nicht aufgeführt ist die Ergänzung der Beschwerdeführerin, wonach Supportfälle über einzelne Webseiten mit einzigartigen URLs abgewickelt würden, da bei www.apfelkiste.ch Bestellungen standardmässig ohne ein Kunden- oder Nutzerkonto möglich seien (Gastbestellungen).

E. 4.5.3

Weiter hält die angefochtene Verfügung unter Bst. A, Ziffer 2.5 fest, von der Datensicherheitsverletzung seien gewisse Datenkategorien betroffen. Dass, wie von der Beschwerdeführerin mit Schreiben vom 12. Mai 2024 der Vorinstanz mitgeteilt, nicht bei allen betroffenen Kundinnen und Kunden alle genannten Datenkategorien betroffen waren, wird in der angefochtenen Verfügung nicht erwähnt. Zudem hält die angefochtene Verfügung, entgegen der Mitteilung der Beschwerdeführerin, die von maximal rund 19'000 einzelnen URLs respektive betroffenen Kundinnen und Kunden spricht, unter Bst. A, Ziffer 2.6 im Wesentlichen fest, es seien mindestens 19'000 betroffene Links respektive Kundinnen und Kunden von der Datensicherheitsverletzung betroffen. Unter Bst. A, Ziffer 2.7 der angefochtenen Verfügung führt die Vorinstanz weiter aus, die Beschwerdeführerin habe nach Feststellung der Datensicherheitsverletzung verschiedene Massnahmen getroffen, um die Nutzung der Links unberechtigten Dritten zu erschweren. Die Konkretisierung der Beschwerdeführerin, wonach die Massnahmen den Zugriff auf Supportfälle durch unberechtigte Dritte verhindern würden, es der Kundschaft jedoch heute noch freistehe, Dritten den Zugriff auf ihre Supportfälle zu ermöglichen, wurde in der angefochtenen Verfügung ebenfalls nicht aufgeführt.

E. 4.5.4

Die angefochtene Verfügung hält in Bst. A, Ziffer 2.8 weiter fest, dass die Beschwerdeführerin in ihrer Meldung angegeben habe, dass die Information der betroffenen Personen einen unverhältnismässigen Aufwand erfordern würde oder allenfalls unmöglich sei. Die Ermittlung der betroffenen Personen via die Links, die in Suchergebnissen ersichtlich seien, sei aufwändig gewesen und die Massnahmen zur Schliessung der Sicherheitslücke sei als vorrangig erachtet worden. Dazu kann festgehalten werden, dass die von der Beschwerdeführerin gemachten Ergänzungen in der angefochtenen Verfügung nicht übernommen wurden. Diese konkretisierten nämlich, dass die Information der einzelnen betroffenen Kundinnen und Kunden nicht möglich gewesen sei, weil für sie die einzelnen URLs im Index der Suchmaschine Bing von Microsoft von Hand hätten ermittelt werden müssen, was Tage oder eher Wochen gedauert hätte. Weiter hielt die Beschwerdeführerin fest, dass in diesem Zeitraum keine Löschung aller URLs im entsprechenden Format habe beantragt werden können. Genauso habe der Zugriff durch und via die Suchmaschine Bing nicht gezielt blockiert werden können, weil in der Folge die URLs von Microsoft als ungültig aus dem Index genommen worden wären. Die Identifizierung der betroffenen Kundschaft sei dabei verworfen worden, weil die Massnahmen zum Schutz der Kundschaft als vorranging erachtet worden seien und nicht weil ihre Ressourcen gebunden worden wären.

E. 4.5.5
Schliesslich führte die Vorinstanz unter Bst. A, Ziffer 2.9 auf, sie habe die Beschwerdeführerin mit E-Mail vom 12. März 2024 gestützt auf Art. 24 Abs. 4 DSG aufgefordert, die betroffenen Personen zu informieren und sie (die Vorinstanz) bis zum 27. März 2024 über die unternommenen Schritte zu orientieren.

E. 4.5.6
Zusammenfassend kann festgehalten werden, dass die Vorinstanz die Ausführungen der Beschwerdeführerin zum Sachverhalt in der angefochtenen Verfügung nicht respektive nur teilweise berücksichtigt hat.

E. 5.1
Nachfolgend ist zu prüfen, ob die von der Beschwerdeführerin gemachten Ausführungen zum Sachverhalt als rechtserheblich im Sinne von Art. 49 VwVG zu qualifizieren sind (vgl. vorstehende E. 2). Rechtserheblich sind alle Tatsachen, von deren Vorliegen es abhängt, ob über den streitigen Anspruch so oder anders zu entscheiden ist (BGE 117 V 282 E. 4a). Im Weiteren ist vorab auf die Datenschutzbestimmungen einzugehen.

E. 5.2.1
Das Datenschutzrecht bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden (Art. 1 DSG). Es gilt für die Bearbeitung von Personendaten natürlicher Personen durch private Personen und Bundesorgane (Art. 2 DSG). Als Personendaten gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (Art. 5 Bst. a DSG). Unter Bearbeiten ist nach Art. 5 Bst. d DSG jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten, zu verstehen.

E. 5.2.2
Die Verletzung der Datensicherheit - auch Data Breach genannt - ist gemäss der Legaldefinition von Art. 5 Bst. h DSG «eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden». Die Verletzung der Datensicherheit lässt sich auch als «planwidrigen Vorfall mit Sicherheitsrelevanz» beschreiben, der zur Beeinträchtigung eines oder mehrerer Schutzziele der Datensicherheit führt. Dabei sind drei Schutzziele massgebend: Vertraulichkeit (die Daten sind nur Berechtigten zugänglich), Verfügbarkeit (die Daten sind verfügbar, wenn sie benötigt werden) und Integrität (die Daten werden nicht unberechtigt oder unbeabsichtigt verändert). Eine Verletzung der Datensicherheit liegt mit anderen Worten vor, wenn mindestens einer dieser drei Aspekte unbeabsichtigt oder widerrechtlich beeinträchtigt wird. Grundsätzlich muss es effektiv zu einer solchen Beeinträchtigung kommen beziehungsweise gekommen sein. Die Vertraulichkeit gilt ohnehin schon als beeinträchtigt, sobald die blosse Möglichkeit besteht, dass Personendaten für Unbefugte zugänglich sind; ob ein entsprechender Zugriff tatsächlich stattfindet beziehungsweise stattgefunden hat, ist irrelevant. Eine Verletzung der Datensicherheit kann unter anderem mit einer dauerhaften Beeinträchtigung sowie einer eigentlichen Persönlichkeitsverletzung einhergehen, indem die betroffene Person etwa die Kontrolle über ihre Daten verliert oder indem die Daten

missbraucht beziehungsweise Unbefugten offengelegt werden. Ob sich eine Verletzung der Datensicherheit ereignet hat, ist unabhängig davon zu beurteilen, ob diese schuldhaft oder widerrechtlich herbeigeführt wurde. Unbeachtlich sind in diesem Zusammenhang auch die mit der Verletzung verbundenen Risiken. Die Verletzung der Datensicherheit kann sowohl durch Dritte als auch durch den Verantwortlichen beziehungsweise Auftragsbearbeiter selbst verursacht werden (zum Ganzen vgl. Mathys/Thomann, in: Blechta/Vasella [Hrsg.], Datenschutzgesetz - Öffentlichkeitsgesetz, Basler Kommentar, 4. Aufl. 2024, [nachfolgend: BSK DSG/BGÖ], N. 9 f. und N. 62 zu Art. 24).

E. 5.2.3

Nach Art. 24 Abs. 1 DSG meldet der Verantwortliche dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Der Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt (Art. 24 Abs. 4 DSG). Die Meldepflicht von Art. 24 Abs. 4 DSG richtet sich an den Verantwortlichen und ist gegenüber der betroffenen Person wahrzunehmen. Vorausgesetzt wird, dass sich eine Verletzung der Datensicherheit ereignet hat. Die betroffene Person muss nur ausnahmsweise über eine Verletzung der Datensicherheit informiert werden. Führt die Verletzung voraussichtlich zu einem hohen Risiko für die betroffene Person, löst dies zwar die Meldepflicht nach Art. 24 Abs. 1 DSG gegenüber dem EDÖB aus; die betroffene Person selbst muss jedoch nicht informiert werden, sofern es zu ihrem Schutz nicht erforderlich ist. Zweck der Meldepflicht von Art. 24 Abs. 4 DSG ist nicht primär das Schaffen von Transparenz; vielmehr geht es darum, dass die betroffene Person, wenn sie selbst tätig werden sollte, in die Lage versetzt wird, sich vor den möglichen Folgen der Verletzung zu schützen oder diese abzumildern. Bei der Beurteilung der Erforderlichkeit besteht ein gewisser Ermessensspielraum (zum Ganzen vgl. Mathys/Thomann, BSK DSG/BGÖ, N. 63 f. zu Art. 24). Nach Art. 24 Abs. 5 DSG kann der Verantwortliche die Information an die betroffene Person einschränken, aufschieben oder darauf verzichten, wenn ein Grund nach Art. 26 Abs. 1 Bst. b oder Abs. 2 Bst. b DSG vorliegt oder eine gesetzliche Geheimhaltungspflicht dies verbietet (Bst. a), die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert (Bst. b) oder die Information der betroffenen Person durch eine öffentliche Bekanntmachung in vergleichbarer Weise sichergestellt ist (Bst. c).

E. 5.3

Nachfolgend ist entsprechend zu prüfen, ob die Ausführungen der Beschwerdeführerin zum Sachverhalt sowohl für die Beurteilung, ob eine Datenschutzverletzung nach Art. 5 Bst. h DSG vorliegt, als auch für die Beurteilung relevant respektive rechtserheblich sind, ob die Beschwerdeführerin die betroffenen Personen über die Datensicherheitsverletzung gemäss Art. 24 Abs. 4 DSG zu informieren hat (es zu ihrem Schutz erforderlich ist) oder ob gemäss Art. 24 Abs. 5 DSG auf eine Information verzichtet werden kann.

E. 5.3.1

Aus den Akten ergibt sich, dass RMA-URLs von Supportfällen der Beschwerdegegnerin in den Index der Suchmaschine Bing von Microsoft gelangten und damit seit ungefähr Juni 2023 Kundendaten respektive Personendaten nach Art. 5 Bst. a DSG, nämlich Kontaktdaten (Namen, E- Mail-Adressen, Postadressen), Kommunikationsinhalte (des Austausches zwischen der Kundschaft und «apfelkiste.ch» zum Supportfall), Bankdaten (IBAN) sowie

Bilddaten (Fotos der gekauften Produkte) und Gutscheincodes Unbefugten offengelegt/zugänglich gemacht wurden respektive die Möglichkeit bestand, dass Personendaten für Unbefugte zugänglich sind. Damit wurde das Schutzziel der Vertraulichkeit beeinträchtigt, ungeachtet dessen, ob ein entsprechender Zugriff tatsächlich stattgefunden hat. Dies stellt nach dem vorstehend unter E. 5.2.2 Ausgeführten eine Datensicherheitsverletzung dar, wobei die mit der Verletzung der Datensicherheit verbunden Risiken unbeachtlich sind.

E. 5.3.2

Für die rechtliche Beurteilung, ob eine Datensicherheitsverletzung vorliegt, ist die Anzahl der von der Datensicherheitsverletzung betroffenen Personen nicht wesentlich. Massgebend ist nicht, ob von der Datensicherheitsverletzung höchstens oder mindestens 19'000 URLs respektive Kundinnen und Kunden betroffen sind, sondern dass Personendaten der einzelnen Kundschaft Unbefugten zugänglich waren respektive die Möglichkeit bestand, dass Personendaten für Unbefugte zugänglich sind. Auch ist nicht entscheidend, ob sämtliche oder nur gewisse Datenkategorien von der Datenschutzverletzung betroffen sind. Gemäss Meldung vom 16. Februar 2024 der Beschwerdeführerin nannte sie Kategorien von Personendaten, die betroffen sind. Für das Vorliegen einer Datenschutzverletzung reicht es aus, dass eine der hiervor genannten Kategorien von Personendaten Unbefugten zugänglich gemacht wurde respektive die Möglichkeit bestand, dass Personendaten für Unbefugte zugänglich waren. Des Weiteren beurteilt sich die Frage, ob eine Datensicherheitsverletzung vorliegt, nicht anders, ob die Personendaten von (unbefugten) Kundinnen und Kunden oder von (unbefugten) Personen im Internet einsehbar waren, ob nur ein kleiner Teil der RMA-URLs betroffen war und ob die RMA-URLs im Index einer oder mehrerer Suchmaschinen auffindbar waren. Auch vermag das von der Beschwerdeführerin vorgebrachte Argument, wonach die von ihr ergriffenen Massnahmen den Zugriff auf Supportfälle durch unberechtigte Dritte verhindern würden, nichts daran zu ändern, dass die Datenschutzverletzung bereits stattgefunden hat. Nachträglich ergriffene technische Massnahmen, die Unbefugten den Zugriff auf die betroffenen Daten aktuell verhindern sollen, vermögen eine bereits erfolgte unbefugte Offenlegung nicht rückwirkend zu beseitigen. Diese Massnahme schliesst nicht aus, dass die zuvor offengelegten Daten bereits zur Kenntnis genommen, gespeichert oder weiterverarbeitet worden sind. Schliesslich wird nicht substanziiert dargelegt und ist auch nicht ersichtlich, inwiefern das von der Beschwerdeführerin zu Bst. A, Ziffer 2.3, 2.7, 2.8 und 2.9 Ausgeführte (vgl. vorstehende E. 4.5.2, 4.5.4 und 4.5.5) einen Einfluss auf die rechtliche Beurteilung hat, ob eine Datensicherheitsverletzung vorliegt. Weiter ist der Beschwerdeführerin zwar zuzustimmen, dass in der angefochtenen Verfügung unrichtig festgehalten wird, die Risikoeinschätzung sei nicht angepasst worden. Dieser Umstand ist für die Beurteilung, ob eine Datensicherheitsverletzung vorliegt, jedoch nicht von Bedeutung. Wie hiervor festgehalten, sind die mit der Verletzung verbundenen Risiken unbeachtlich (vgl. vorstehende E. 5.2.2). Nach dem Gesagten haben die von der Beschwerdeführerin gerügten Umstände respektive die Ausführungen der Beschwerdeführerin zum Sachverhalt keinen Einfluss auf die rechtliche Beurteilung, ob eine Datenschutzverletzung vorliegt.

E. 5.3.3

Das Argument der Beschwerdeführerin, es sei unbekannt, ob die betroffene Kundschaft im Rahmen ihrer Einwilligung der Nutzung von Microsoft-Produkten auch in die Bearbeitung ihrer Daten für die Suchmaschine Bing und deren Index eingewilligt hätten und dadurch

jegliche Verletzung der Datensicherheit entfallen würde, geht fehl. Suchmaschinen können lediglich Inhalte indexieren, die sie abrufen können. Konnte ein Crawler, wie vorliegend jener von Bing, den Link öffnen, dann weil er technisch öffentlich war und zum Beispiel nicht ausreichend abgesichert oder nicht gegen Indexierung geschützt war. Die Verantwortung dafür kann die Beschwerdeführerin nicht auf eine allfällige Einwilligung der Kundschaft im Rahmen ihrer Nutzung von Microsoft-Produkten und gegebenenfalls auch in die Bearbeitung ihrer Daten für die Suchmaschine und deren Index abwälzen. Der Vorinstanz ist zuzustimmen, wenn sie vorbringt, die Beschwerdeführerin habe schliesslich selbst den Zugriff des Suchmaschinen-Crawlers im Nachgang blockiert, eine Massnahme, welche die Kundschaft selbst nicht hätten vornehmen können. Dass der Suchmaschinen-Crawler die RMA-URLs, die eigentlich nur für die (berechtigte) Kundschaft bestimmt ist, durchsuchen und indexieren konnte, stellt ein Konfiguration- oder Sicherheitsproblem der Beschwerdeführerin dar und hat nichts mit der allfälligen Einwilligung im Rahmen der Nutzung von Microsoft-Produkten zu tun.

E. 5.3.4

Für die Beurteilung der Frage, ob die betroffenen Personen über die Datensicherheitsverletzung zu informieren sind, ist massgebend, ob ein Schutzbedarf der betroffenen Personen besteht (vgl. vorstehende E. 5.2.3). Wie nachstehend noch zu zeigen sein wird (vgl. nachstehende E. 6.1.3), besteht ein Schutzbedarf der von der Datensicherheitsverletzung betroffenen Personen. An der Beurteilung, ob ein Schutzbedarf besteht, vermögen die Umstände, dass lediglich ein kleiner Teil der RMA-URLs betroffen und höchstens und nicht mindestens 19'000 URLs respektive Kundinnen und Kunden betroffen sind, nichts zu ändern. Der Schutzbedarf bezieht sich auf die einzelne von der Datenschutzverletzung betroffene Kundschaft und besteht darin, die Massnahmen ergreifen zu können, um die Risiken für deren Persönlichkeit oder Grundrechte zu reduzieren. Diese zu ergreifenden Massnahmen hängen damit nicht von der Anzahl der betroffenen RMA-URLs respektive Kundschaft ab. Auch ändert nichts am Schutzbedarf der betroffenden Personen, ob die Personendaten lediglich von Unbefugten im Internet eingesehen werden können. Nicht ideal ist die unpräzise Formulierung in der angefochtenen Verfügung, wonach Supportfälle im Internet einsehbar waren. Damit wird nämlich suggeriert, jedermann habe grundsätzlich Zugriff auf die Personendaten der von der Datenschutzverletzung Betroffenen, obwohl es sich um einen abgeschlossen Empfängerkreis handelt (19'000 unbefugte Dritte respektive Kundinnen und Kunden der Beschwerdeführerin). Dies ist jedoch insofern nicht relevant, als dass dieser Empfängerkreis der Personendaten als anonymer Empfängerkreis zu behandeln ist, da er nicht mehr identifiziert werden kann. Entsprechend besteht - wie dies der Fall wäre, wenn die Supportfälle im Internet (öffentlich) einsehbar wären - keine Möglichkeit, das Verhalten der unbefugten Dritten einzuschätzen oder zu kontrollieren. Mit der fehlenden Identifizierbarkeit geht ein Kontrollverlust einher. Selbst wenn das Missbrauchsrisiko grundsätzlich mit steigender Anzahl Personen, die (unbefugt) Zugriff auf die Personendaten haben, steigt, so handelt es sich vorliegend beim Kundenkreis um einen nicht unbedeutenden Empfängerkreis (rund 19'000 Personen). Ein Datenmissbrauch kann nicht ausgeschlossen werden; vielmehr besteht ein relevantes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen. Der Umstand, dass bekannt ist, dass es sich um Kundschaft der Beschwerdeführerin handelt, vermag das Risiko des Datenmissbrauchs nicht zu mindern und ändert folglich weder etwas am Schutzbedarf der betroffenen Personen noch an den von ihnen zu ergreifenden Massnahmen. Inwiefern der eingangs

erwähnten mangelnden Präzision des Sachverhaltes Relevanz zukommen soll, ist deshalb nicht ersichtlich. Dass die RMA-URLs lediglich im Index einer einzigen Suchmaschine auffindbar waren, ist insoweit von Bedeutung, als die Risikobeurteilung nicht mit jener bei einer Indexierung durch mehrere Suchmaschinen gleichzusetzen ist. Die Auffindbarkeit der Personendaten und damit das Risiko eines Datenmissbrauchs ist bei einer Indexierung im zweiten Fall grundsätzlich höher einzustufen. Ungeachtet dessen besteht aber auch bei einer Auffindbarkeit über lediglich eine Suchmaschine ein relevantes Risiko des Datenmissbrauchs und damit eine Gefährdung der Persönlichkeit sowie der Grundrechte der betroffenen Personen. Die in diesem Zusammenhang zu ergreifenden Massnahmen sind hingegen in beiden Konstellationen dieselben. Des Weiteren ist für die Beurteilung des Schutzbedarfs nicht ausschlaggebend, ob bei den betroffenen Kundinnen und Kunden nur einzelne, mehrere oder sämtliche genannten Datenkategorien betroffen sind. Massgeblich ist vielmehr, ob die konkret betroffenen Personendaten geeignet sind, die Persönlichkeit und die Grundrechte der betroffenen Personen zu beeinträchtigen, sowie welches Missbrauchs- und Schadenspotenzial mit ihrer unbefugten Offenlegung verbunden ist. Auch der unbefugte Zugriff auf eine einzelne Datenkategorie kann grundsätzlich ein erhebliches Risiko für die betroffenen Personen begründen. Der Schutzbedarf bestimmt sich daher nach der potenziellen Eingriffsintensität sowie dem damit verbundenen Risiko und nicht nach der Anzahl der betroffenen Datenkategorien. Entsprechend bleibt der Schutzbedarf auch dann unverändert, wenn lediglich eine Datenkategorie betroffen ist. Das Argument der Beschwerdeführerin, wonach die von ihr ergriffenen Massnahmen den Zugriff auf Supportfälle durch unberechtigte Dritte verhindern würden (Ziffer 2.7), ändert - wie bereits ausgeführt (vgl. E. 5.3.2) - nichts daran, dass die betreffenden Daten zuvor unberechtigten Kundinnen und Kunden zugänglich gemacht beziehungsweise offengelegt wurden und damit eine Datenschutzverletzung vorliegt. Zudem ist nicht ausgeschlossen, dass die zuvor offengelegten Daten bereits zur Kenntnis genommen, gespeichert oder weiterverarbeitet worden sind. Entsprechend besteht auch nach der nachträglichen Zugriffsbeschränkung weiterhin ein relevantes Risiko eines Datenmissbrauchs, weshalb der Schutzbedarf der betroffenen Personen fortbesteht. Inwiefern schliesslich das von der Beschwerdeführerin zu Bst. A, Ziffern 2.3, 2.8 und 2.9 der angefochtenen Verfügung Ausgeführte einen Einfluss auf die rechtliche Beurteilung des Vorliegens eines Schutzbedarfs hat, wird nicht näher substantiiert und ist auch nicht ersichtlich. Die Begründung der Beschwerdeführerin, wonach keine Anzeichen dafür bestanden hätten, dass sich mögliche Folgen für die betroffene Kundschaft tatsächlich manifestiert hätten, vermag nicht zu überzeugen. Dasselbe gilt betreffend den Einwand, es habe weder eine relevante Eintrittswahrscheinlichkeit bestanden noch habe sich eine solche - entgegen den anfänglichen Erwartungen - als gering erwiesen, zumal keine Rückmeldungen von Kundinnen und Kunden erfolgt seien. Der Umstand, dass - soweit bekannt - bisher keine konkreten Folgen eingetreten sind, erlaubt keinen Schluss darauf, dass das Risiko als gering einzustufen wäre. Ebenso kann der Beschwerdeführerin nicht gefolgt werden, wenn sie die Eintrittswahrscheinlichkeit eines Schadens davon abhängig macht, ob sich die betroffene Kundschaft gemeldet hat oder nicht. Folglich hat auch der Umstand, dass in der angefochtenen Verfügung unzutreffend festgehalten wird, die Risikoeinschätzung sei nicht angepasst worden, im Ergebnis keinen Einfluss auf die Frage, ob ein Schutzbedarf besteht. Nach dem Gesagten haben die von der Beschwerdeführerin gerügten Umstände respektive deren Ausführungen zum Sachverhalt keinen Einfluss auf die rechtliche Beurteilung der Frage, ob die betroffenen Personen über die Datensicherheitsverletzung zu informieren

sind.

E. 5.3.5

Dass - wie die Beschwerdeführerin geltend macht - lediglich ein kleiner Teil der RMA-URLs betroffen ist, dass höchstens und nicht mindestens 19'000 URLs respektive Kundinnen und Kunden betroffen sind und die Personendaten lediglich von (unbefugter) Kundschaft und nicht von (unbefugten) Personen im Internet eingesehen werden konnten, ist für die Beurteilung der Frage, ob ein Ausnahmegrund nach Art. 24 Abs. 5 DSG vorliegt, um die Information der betroffenen Personen einzuschränken, aufzuschieben oder darauf zu verzichten, nicht massgebend. Dasselbe gilt für den Einwand, dass nicht sämtliche, sondern nur gewisse Datenkategorien von der Datenschutzverletzung betroffen seien und die RMA-URLs im Index einer und nicht mehrerer Suchmaschinen auffindbar waren. Inwiefern das von der Beschwerdeführerin zu Bst. A, Ziffer 2.3, 2.7 und 2.9 Ausgeführte (vgl. vorstehende E. 4.5.2, 4.5.3, 4.5.5) einen Einfluss auf die rechtliche Beurteilung hat, ob eine Ausnahme von der Informationspflicht nach Art. 24 Abs. 4 DSG vorliegt, wird nicht substanziiert dargelegt und ist auch nicht ersichtlich. Dass in der angefochtenen Verfügung unrichtig festgehalten wird, die Risikoeinschätzung sei nicht angepasst worden, ist für diese Beurteilung ebenfalls nicht von Bedeutung. Die Beschwerdeführerin moniert schliesslich, die Vorinstanz habe den Sachverhalt betreffend die Identifizierung der von der Datenschutzverletzung betroffenen Kundschaft in Bst. A, Ziffer 2.8 falsch festgehalten. Sie führt aus, dass die Information einzelner betroffener Kundinnen und Kunden nicht möglich gewesen sei, weil für die Identifizierung der einzelnen Kundschaft die einzelnen URLs im Index der Suchmaschine Bing von Microsoft von Hand hätten ermittelt werden müssen, was Tage oder eher Wochen gedauert hätte. In diesem Zeitraum hätte keine Löschung aller URLs im entsprechenden Format beantragt werden können. Genauso wenig hätte der Zugriff durch und via die Suchmaschine Bing gezielt blockiert werden können, weil in der Folge die URLs von Microsoft als ungültig aus dem Index genommen worden wären. Die Identifizierung der betroffenen Kundschaft sei dabei verworfen worden, weil die Massnahmen zum Schutz der Kundinnen und Kunden als vorrangig erachtet worden seien und nicht weil ihre Ressourcen gebunden worden wären. Die Verfügung hält diesbezüglich fest, dass die Beschwerdeführerin in ihrer Meldung angegeben habe, dass die Information der betroffenen Personen einen unverhältnismässigen Aufwand erfordern würde oder allenfalls unmöglich sei. Die Ermittlung der betroffenen Personen via die Links, die in Suchergebnissen ersichtlich seien, wäre aufwändig gewesen und die Massnahmen zur Schliessung der Sicherheitslücke sei als vorrangig erachtet worden.

E. 5.3.6

Dass die Vorinstanz diesen Teil des Sachverhalts falsch festgehalten haben soll, ist nicht ersichtlich. Ihr kann einzig vorgeworfen werden, ihn unpräzise formuliert zu haben. Dies ändert jedoch nichts an der rechtlichen Beurteilung der Frage, ob eine Ausnahme von der Informationspflicht nach Art. 24 Abs. 4 DSG vorliegt. Beide in der Verfügung genannten Gründe - die Unmöglichkeit und die Unverhältnismässigkeit - sind als Ausnahmegründe in Art. 24 Abs. 5 DSG vorgesehen.

E. 5.4

Zusammenfassend ist festzuhalten, dass die von der Beschwerdeführerin gemachten Ausführungen keine Elemente des rechtserheblichen Sachverhalts im Sinne von Art. 49 VwVG betreffen und daher nicht entscheidwesentlich sind. Inwiefern die Vorinstanz den

rechtserheblichen Sachverhalt unrichtig oder unvollständig festgestellt haben soll, ist nicht ersichtlich. Die diesbezügliche Rüge ist demnach unbegründet.

E. 6.1.1

Die Beschwerdeführerin rügt sodann die Verletzung von Bundesrecht und begründet dies im Wesentlichen damit, es bestehe entgegen der Ansicht der Vorinstanz kein Schutzbedarf der betroffenen Personen gemäss Art. 24 Abs. 4 DSG. Die Vorinstanz verweise lediglich pauschal und ohne konkreten Bezug zur vorliegenden Angelegenheit auf Phishing als Gefahr. Sie selbst habe Phishing in ihrer Meldung nicht als mögliche Folge der Verletzung der Datensicherheit identifiziert. Dies deshalb, weil Phishing eine alltägliche und dauerhafte Gefahr für Nutzerinnen und Nutzer darstelle, unabhängig von der vorliegenden Angelegenheit. Schliesslich sei mit Blick auf den Zeitablauf eine allfällige risikomindernde Wirkung nicht mehr zu erwarten.

E. 6.1.2

Die Vorinstanz ist der Auffassung, es bestehe ein Schutzbedarf. Sie führt aus, bei der Information der betroffenen Personen handle es sich um eine gesetzliche Verpflichtung, sofern die Voraussetzungen erfüllt seien. Die Information solle den betroffenen Personen ermöglichen, die Kontrolle über die Nutzung ihrer Daten auszuüben. Sie führt aus, die Beschwerdeführerin habe in ihrer Meldung vom 16. Februar 2024 den Identitätsdiebstahl und einen finanziellen Schaden als mögliche Konsequenz für die betroffenen Personen aufgeführt. Oftmals würden Datensätze aus Datensicherheitsverletzungen für die in der angefochtenen Verfügung beschriebenen Phishing-Attacken verwendet. Die Vorinstanz moniert zudem, dass die Beschwerdeführerin geltend mache, dass eine risikomindernde Wirkung aufgrund des Zeitablaufs nicht mehr erwartet werden könne, obwohl sie eine Verzögerung der Information selbst herbeigeführt habe. Mit diesem Argument werde die Informationspflicht ausgehöhlt.

E. 6.1.3

Wie vorstehend in E. 5.3.1 erwähnt, wurden Personendaten nach Art. 5 Bst. a DSG, nämlich Kontaktdaten (Namen, E- Mail-Adressen, Postadressen), Kommunikationsinhalte (des Austausches zwischen der Kundschaft und «apfelkiste.ch» zum Supportfall), Bankdaten (IBAN) sowie Bilddaten (Fotos der gekauften Produkte) und Gutscheincodes Unbefugten offengelegt respektive zugänglich gemacht. Es stellt sich die Frage, ob die durch die Datenschutzverletzung bestehenden Risiken durch die Information der betroffenen Personen verhindert oder reduziert werden können. Dies ist insbesondere der Fall, wenn die betroffene Person selbst in der Lage ist, bestimmte Massnahmen zu ihrem Schutz zu treffen. Nicht erforderlich ist eine Information zum Schutze der betroffenen Person hingegen dann, wenn sich die negativen Folgen bereits verwirklicht haben oder wenn die betroffene Person nichts Relevantes (mehr) dagegen ausrichten kann. Der EDÖB darf die Information auch nur anfordern, wenn es zum Schutz der betroffenen Person erforderlich ist (Mathys/Thomann, BSK DSG/BGÖ, N. 63, 66 und 68 zu Art. 24). Von der Datensicherheitsverletzung sind vorliegend diverse Personendaten betroffen. In Kombination mit der IBAN, dem Namen und der Adresse einer Person kann insbesondere Identitäts- oder Social-Engineering-Betrug begangen werden. Auch könnte zum Beispiel mittels eines Lastschriftverfahrens Geld bezogen werden. Als Massnahmen, welche die betroffene Person selbst ergreifen kann, kommen beispielsweise die Änderung von Zugangsdaten beziehungsweise Passwörtern zu Benutzerkonten, die Prüfung von

Kontoauszügen, die kritische Prüfung von Nachrichten und Anfragen, welche möglicherweise mit widerrechtlich beschafften (besonders vertraulichen) Personendaten fabriziert wurden und Phishing-Zwecken dienen könnten, in Betracht (Mathys/Thomann, BSK DSG/BGÖ, N. 66 und 67 zu Art. 24). Die betroffene Person könnte beispielsweise diese Massnahmen ergreifen oder die Information der eigenen Bank und das Einschränken oder Sperren des Lastschriftverfahrens vornehmen. Ein Schutzbedarf der betroffenen Personen liegt entsprechend vor, weshalb sich die Information der betroffenen Personen als notwendig erweist (Art. 24 Abs. 4 DSG).

E. 6.1.4

Das von der Beschwerdeführerin vorgebrachte Argument, wonach aufgrund des Zeitablaufs eine risikomindernde Wirkung nicht mehr zu erwarten sei, verfängt nicht. Die seit der Datenschutzverletzung verstrichene Zeit schliesst einen Missbrauch der betroffenen Daten nicht aus. Personendaten können nach einer unbefugten Offenlegung jederzeit gespeichert, kopiert und zu einem späteren Zeitpunkt weiterverwendet oder weitergegeben werden. Ein Missbrauch kann demnach auch lange nach der unbefugten Offenlegung respektive der Datenschutzverletzung erfolgen. Der Zeitablauf lässt daher keinen verlässlichen Schluss zu, dass die betroffenen Daten nicht (mehr) missbräuchlich verwendet werden und eine risikomindernde Wirkung nicht mehr zu erwarten wäre. Entsprechend bleibt das Risiko eines Datenmissbrauchs - und damit der Schutzbedarf der betroffenen Personen - ungeachtet der seit der Datenschutzverletzung vergangenen Zeit bestehen.

E. 6.2.1

Die Beschwerdeführerin bringt weiter vor, sie habe sich für den Schutz aller betroffenen Personen entschieden und alle möglicherweise betroffenen URL's bei der Suchmaschine Bing von Microsoft blockieren lassen. Dadurch sei es heute jedoch technisch unmöglich, über die Suchmaschine Bing - ohne diese gehe es nicht - die betroffene Kundschaft ausfindig zu machen. Mit der Anordnung der Vorinstanz, die von der Datensicherheitsverletzung betroffenen Personen zu informieren, verlange sie objektiv Unmögliches. Die Vorinstanz verweise in der angefochtenen Verfügung zwar auf die Möglichkeit der öffentlichen Bekanntmachung, führe jedoch aus, es seien keine Ausnahmen der Informationspflicht gestützt auf Art. 24 Abs. 5 DSG ersichtlich. Entsprechend sei die Möglichkeit einer öffentlichen Bekanntmachung nicht Gegenstand der Beschwerde.

E. 6.2.2

Die Vorinstanz macht geltend, Art. 24 Abs. 5 Bst. c DSG hebe die Pflicht zur Information der betroffenen Personen nicht auf, sondern modifiziere sie, indem die Möglichkeit der öffentlichen Bekanntmachung zur Verfügung gestellt werde. Sie führt weiter aus, dass auch eine Information aller Kundinnen und Kunden denkbar sei, wenn die individualisierte Kommunikation nicht möglich oder unverhältnismässig sei. Sie führt weiter aus, dass die Unmöglichkeit, die betroffene Kundschaft ausfindig zu machen, erst durch das Ergreifen der technischen Massnahmen durch die Beschwerdeführerin entstanden sei, um den Zugang durch unberechtigte Personen zu unterbinden. Dabei stelle sich die Frage, ob ein derartiges Vorgehen die Beschwerdeführerin als Verantwortliche von ihrer Informationspflicht entbinden könne.

E. 6.2.3

Es kann festgehalten werden, dass die Vorinstanz in der angefochtenen Verfügung festhält, dass die Information der von der Datensicherheitsverletzung betroffenen Kundschaft nicht unmöglich sei. Da alle betroffenen Personen Kundinnen und Kunden der Beschwerdeführerin seien, könnten diese von ihr identifiziert werden. Diese Kundinnen und Kunden stünden mit der Beschwerdeführerin betreffend eines Kaufes im Austausch, weshalb ihre Kontaktdaten vorhanden seien. Die Beschwerdeführerin habe weder in ihrer Meldung (vom 16. respektive 25. Februar 2024) noch in ihrer E-Mail vom 21. März 2024 konkrete Gründe genannt, weshalb eine Information der betroffenen Kundschaft unmöglich sei. Sie habe jedoch geltend gemacht, dass deren Identifikation aufwändig sei, da diese anhand der über die Suchmaschine auffindbaren Links identifiziert werden müsste. Die Vorinstanz weist in der angefochtenen Verfügung darauf hin, dass ein unverhältnismässiger Aufwand vorliegen könne, wenn bei einer grossen Anzahl Betroffener jede und jeder Einzelne informiert werden müsse. In derartigen Fällen könne der organisatorische und finanzielle Aufwand im Verhältnis zum Informationsgewinn der betroffenen Personen im Ungleichgewicht sein. Dies möge im vorliegenden Fall zutreffen, da die Anzahl der betroffenen Personen auf 19'000 geschätzt werde und der Aufwand, diese einzeln zu identifizieren nicht unerheblich sei. Damit könne Art. 25 Abs. 5 Bst. c DSG zur Anwendung gelangen, der es dem Verantwortlichen erlaube, die betroffenen Personen durch eine öffentliche Bekanntmachung zu informieren, wenn sie dadurch auf vergleichbare Weise informiert würden. Damit seien keine Gründe nachgewiesen worden, die eine Einschränkung der Information der Betroffenen rechtfertigen würden. Eine Information der Betroffenen sei vorliegend angezeigt. Mit der Meldung vom 16. Februar 2024 informierte die Beschwerdeführerin die Vorinstanz unter anderem über die von ihr ergriffenen Massnahmen. Sie teilte mit, sie habe insbesondere den Crawler von Bing für RMA- URLs blockiert und bei Bing das Blockieren beziehungsweise das Löschen aller URLs im Format der RMA-URLs beantragt. Mit Schreiben vom 12. Mai 2024 teilte die Beschwerdeführerin der Vorinstanz mit, die Identifizierung der betroffenen Kundschaft sei verworfen worden, weil sie die Massnahmen zum Schutz dieser als vorrangig erachtet habe. Gemäss Art. 24 Abs. 1 DSG meldet der Verantwortliche dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. In der Meldung nennt er mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen (Art. 24 Abs. 2 DSG). Dabei geht es um Massnahmen, welche die Verletzung beseitigen oder deren Folgen mildern (vgl. Botschaft vom 15. September 2017 über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBI 2017 6941, 7064, 7065). Dass die Beschwerdeführerin diverse Massnahmen ergriffen hat, um die Datensicherheitsverletzung umgehend zu beheben und die Folgen der Datensicherheitsverletzung zu minimieren, ist nicht zu beanstanden. Vielmehr kann erwartet werden, dass im Falle einer Datensicherheitsverletzung unverzüglich alle zumurbaren und geeigneten Massnahmen ergriffen werden, um einen (weiteren) Schaden abzuwenden und die Auswirkungen so gering wie möglich zu halten. Ein derartiges Vorgehen stellt somit nicht nur ein korrektes, sondern gebotenes Vorgehen dar.

E. 6.3

Nachfolgend ist zu prüfen, ob eine gesetzlich vorgesehene Ausnahme vorliegt, um die Information der betroffenen Personen einzuschränken, aufzuschieben oder darauf zu verzichten.

E. 6.3.1

Nach Art. 24 Abs. 5 DSG kann der Verantwortliche die Information an die betroffene Person einschränken, aufschieben oder darauf verzichten, wenn ein Grund nach Art. 26 Abs. 1 Bst. b oder Abs. 2 Bst. b DSG vorliegt oder eine gesetzliche Geheimhaltungspflicht dies verbietet (Bst. a), die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert (Bst. b) oder die Information der betroffenen Person durch eine öffentliche Bekanntmachung in vergleichbarer Weise sichergestellt ist (Bst. c).

E. 6.3.2

Dass ein Einschränkungsgrund nach Art. 24 Abs. 5 Bst. a DSG i.V.m. Art. 26 Abs. 1 Bst. b DSG gegeben ist, wonach überwiegende Interessen Dritter vorliegen, ist nicht ersichtlich und ein solcher wird auch nicht geltend gemacht.

E. 6.3.3

Der Ausnahmetatbestand gemäss Art. 24 Abs. 5 Bst. a DSG i.V.m. Art. 26 Abs. 2 Bst. b DSG findet nur Anwendung, sofern es sich beim Verantwortlichen um ein Bundesorgan handelt; diese Ausnahmebestimmung ist vorliegend nicht anwendbar.

E. 6.3.4

Auch kommt die Einschränkung gemäss Art. 24 Abs. 5 Bst. a DSG, wonach eine gesetzliche Geheimhaltungspflicht die Information verbietet, vorliegend nicht zur Anwendung. Eine gesetzliche Geheimhaltungspflicht ist nicht gegeben und eine solche wird auch nicht geltend gemacht.

E. 6.3.5

Weiter kommt eine Einschränkung der Meldung an die betroffene Person gemäss Art. 24 Abs. 5 Bst. b DSG zunächst dann in Betracht, wenn eine Information unmöglich ist. Dies trifft insbesondere auf Fälle zu, in denen der Verantwortliche gar nicht weiss, welche Personen von der Verletzung der Datensicherheit betroffen sind, was zum Beispiel darauf zurückzuführen sein kann, dass die Logfiles, aus denen dies ersichtlich wäre, nicht mehr vorhanden sind. Unmöglich ist die Information sodann, wenn sich zwar die betroffenen Personen eruieren lassen, deren Kontaktangaben aber nicht bekannt sind. Allerdings kann sich der Verantwortliche nicht mit dem Argument, er wisse nicht genau, von welchen Personen seiner Kundschaft die Daten gestohlen wurden, der Meldepflicht entziehen. In solchen Konstellationen drängt sich eine «überschiessende» Meldung auf, indem der Verantwortliche auch Personen informiert (und diese beispielsweise zur Änderung von Passwörtern auffordert), die möglicherweise gar nicht von der Verletzung der Datensicherheit betroffen sind. Vorbehalten bleibt die allfällige Anwendbarkeit anderer Ausnahmetatbestände (zum Ganzen vgl. Mathys/Thomann, in: Blechta/Vasella [Hrsg.], a.a.O. N. 89 zu Art. 24). Eine Einschränkung nach Art. 24 Abs. 5 Bst. b DSG ist auch möglich, wenn die Information einen unverhältnismässigen Aufwand erfordert. Von einem solchen ist zum Beispiel auszugehen, wenn eine grosse Anzahl betroffener Personen individuell informiert werden müsste, wobei die dadurch entstehenden Kosten im Verhältnis zum Informationsgewinn für die einzelnen Personen unverhältnismässig wären. Zu denken ist weiter an den Fall, in dem die Kontaktdaten einer grossen Anzahl betroffener Personen nur schwer ermittelbar sind beziehungsweise hierfür langwierige Abklärungen erforderlich wären, so dass die Meldung erst zu einem Zeitpunkt erfolgen könnte, in welchem es zur Vornahme von Gegenmassnahmen durch die betroffenen Personen bereits

zu spät ist, namentlich weil sich das Risiko zwischenzeitlich verwirklicht hat (zum Ganzen vgl. Mathys/Thomann, in: Blechta/Vasella [Hrsg.], a.a.O. N. 90 zu Art. 24).

E. 6.3.6

Vorliegend ist eine Identifikation der betroffenen Personen aufgrund der von der Beschwerdeführerin getroffenen Massnahmen nicht mehr möglich. Doch selbst wenn eine solche möglich wäre, so würde die Einschränkung nach Art. 24 Abs. 5 Bst. b DSG zur Anwendung gelangen, da die Information der betroffenen 19'000 Kundinnen und Kunden einen unverhältnismässigen Aufwand bedeuten würde.

E. 6.3.7

Ist eine Information an die betroffene Person unmöglich oder erfordert sie einen unverhältnismässigen Aufwand, kann stattdessen eine öffentliche Bekanntmachung erfolgen (vgl. Art. 24 Abs. 5 Bst. c DSG). Mit «in vergleichbarer Weise sichergestellt» ist gemeint, dass «die Information der betroffenen Person durch eine individuelle Information nicht substanziell verbessert wird». Demzufolge muss geprüft werden, ob die öffentliche Bekanntmachung ähnlich wirksam ist wie eine individuelle Meldung an die betroffene Person. Nur dann, wenn dies zutrifft, vermag die öffentliche Bekanntmachung eine individuelle Information zu ersetzen. Allerdings statuiert das DSG keine (ausdrückliche) Pflicht, in solchen Fällen eine öffentliche Bekanntmachung vorzunehmen. Dies erscheint insoweit vertretbar, als in Konstellationen, in denen nur vereinzelte betroffene Personen nicht individuell informiert werden können, weil z. B. deren E-Mail-Adressen unbekannt sind, eine öffentliche Bekanntmachung unverhältnismässig erschiene. Allerdings sind in Einzelfällen auch stossende Ergebnisse denkbar: Sind etwa zahlreiche Personen von einer Verletzung der Datensicherheit betroffen und würde deren individuelle Information einen unverhältnismässigen Aufwand erfordern, ist eine öffentliche Bekanntmachung nach dem Gesetzeswortlaut im Prinzip selbst dann nicht erforderlich, wenn dadurch den aus der Verletzung herrührenden Risiken wirksam begegnet werden könnte. Auch fehlt es dem EDÖB in solchen Fällen an der Kompetenz, vom Verantwortlichen (formell) die Vornahme einer öffentlichen Bekanntmachung zu verlangen, weil der EDÖB im Rahmen einer verwaltungsrechtlichen Massnahme grundsätzlich nur ein Verhalten einfordern kann, zu dem der Verantwortliche bereits von Gesetzes wegen verpflichtet ist. Immerhin könnte der EDÖB unter gegebenen Voraussetzungen von sich aus die Öffentlichkeit «über seine Feststellungen und Verfügungen» informieren (Art. 57 Abs. 2 DSG). Um einer solchen Massnahme zuvorzukommen, dürfte dem Verantwortlichen faktisch trotz fehlender (ausdrücklicher) Pflicht regelmässig geraten sein, von sich aus eine öffentliche Bekanntmachung vorzunehmen, soweit dies zum Schutz der betroffenen Personen sinnvoll und im Sinne einer Gesamtbetrachtung verhältnismässig erscheint (zum Ganzen vgl. Mathys/Thomann, in: Blechta/Vasella [Hrsg.], a.a.O. N. 91 und 93 zu Art. 24). In Anwendung des Verhältnismässigkeitsgrundsatzes ist stets die mildeste geeignete Form der Einschränkung zu wählen. Demnach sind etwa eine öffentliche Bekanntmachung, ein Aufschub oder eine Information mit eingeschränkten Angaben gegenüber einem gänzlichen Verzicht vorzuziehen. Sofern ein hohes Risiko vorliegt und die Information tatsächlich einen wesentlichen Beitrag zur Risikominimierung leisten kann, ist schliesslich für eine zurückhaltende Anwendung der Einschränkungsgründe nach Art. 24 Abs. 5 DSG zu plädieren (vgl. Bieri/Powell, in: Bieri/Powell [Hrsg.], Kommentar zum schweizerischen Datenschutzgesetz mit weiteren Erlassen, 2023, N. 25 zu Art. 24 DSG).

E. 6.3.8

Dem Schreiben vom 12. Mai 2024 der Beschwerdeführerin ist zu entnehmen, dass diese der Vorinstanz im Wesentlichen mitgeteilt hat, dass die Information der betroffenen Kundschaft nicht möglich gewesen sei, weil für deren Identifizierung die einzelnen URLs im Index der Suchmaschine Bing von Microsoft von Hand hätte ermittelt werden müssen, was Tage oder eher Wochen gedauert hätte. In diesem Zeitraum hätte keine Löschung aller URLs im entsprechenden Format beantragt werden können. Genauso hätte der Zugriff durch und über die Suchmaschine Bing nicht gezielt blockiert werden können, weil in der Folge die URLs von Microsoft als ungültig aus dem Index genommen worden wären. Weiter teilte sie mit, dass eine Information in allgemeiner Form auf ihrer Internetseite nicht verhältnismässig gewesen wäre. Mit Vernehmlassung vom 15. Oktober 2024 führt die Beschwerdeführerin aus, weshalb sie eine öffentliche Bekanntmachung als unverhältnismässig erachtet. Sie macht geltend, dass mit einer Bekanntmachung auf ihrer Homepage mindestens hunderttausende (potenzielle) Kundinnen und Kunden angesprochen würden, die nicht von der Datenschutzverletzung betroffen seien. Gleichzeitig sei die Wahrscheinlichkeit, dass die bis zu 19'000 betroffenen Kundinnen und Kunden mit der Bekanntmachung erreicht würden, gering. Die Internetseite zähle pro Monat rund 1.5 Millionen aktive Nutzerinnen und Nutzer. Die öffentliche Bekanntmachung sei bei Weitem nicht ähnlich wirksam wie eine individuelle und direkte Meldung an die einzelnen betroffenen Personen. Gleichzeitig würde die nicht betroffene Kundschaft durch die öffentliche Bekanntmachung erheblich und ohne Not verunsichert. Entsprechend sei die öffentliche Bekanntmachung offensichtlich weder geeignet noch zumutbar, selbst wenn die bestrittene Information grundsätzlich erforderlich sei. Da die Vorinstanz die Beschwerdeführerin nicht verpflichten durfte, eine öffentliche Bekanntmachung vorzunehmen (vgl. vorstehende E. 6.3.7), ist diese Möglichkeit richtigerweise lediglich in den Erwägungen der angefochtenen Verfügung enthalten. Der Vorinstanz ist beizupflichten, dass grundsätzlich eine Informationspflicht gemäss Art. 24 Abs. 4 DSG besteht. Wie oben (vgl. E. 6.3.6) gezeigt wurde, erweist sich eine direkte Information vorliegend als unmöglich respektive unverhältnismässig (vgl. Art. 24 Abs. 5 Bst. a DSG). An ihre Stelle kann jedoch eine öffentliche Bekanntmachung im Sinne von Art. 24 Abs. 5 Bst. c DSG treten. Demnach kann die Information der betroffenen Person eingeschränkt, aufgeschoben oder darauf verzichtet werden, wenn die Information durch eine öffentliche Bekanntmachung in vergleichbarer Weise sichergestellt ist. Eine individuelle Information zeichnet sich durch die gezielte Zustellung an die konkrete betroffene Person aus. Ist eine solche Zustellung faktisch ausgeschlossen, kann das in Art. 24 Abs. 5 Bst. c DSG geforderte Erfordernis der «vergleichbaren Weise» nicht dahingehend verstanden werden, dass dieselbe Informationsart verlangt wird. Andernfalls liefe die gesetzlich vorgesehene Ersatzmöglichkeit ins Leere. Der Gesetzgeber hat mit dieser Bestimmung gerade für Fälle faktischer Unmöglichkeit eine alternative Form der Information vorgesehen (vgl. vorstehende E. 6.3.7). Wenn - wie hier - die individuelle Information von vornherein unmöglich ist, wird die Information der betroffenen Person durch eine individuelle Information im Verhältnis zur öffentlichen Bekanntmachung gerade nicht substanziell verbessert (vgl. vorstehende E. 6.3.7 und Bieri/Powell, in: Bieri/Powell [Hrsg.], a.a.O., N. 23 zu Art. 24 DSG). Im Gegenteil können die durch die öffentliche Bekanntmachung erreichten betroffenen Personen die erforderlichen Schutzmassnahmen ergreifen. Mit einer öffentlichen Bekanntmachung zum Beispiel auf der Internetseite der Beschwerdeführerin würde ein Informationskanal gewählt, bei dem damit gerechnet werden darf, dass er zumindest von einem Teil der betroffenen Kundschaft erreicht wird und diese

Informationen über diverse Kanäle (mündliche Weitergabe, Information über Medien usw.) weitergetragen werden, sodass schliesslich auch jene betroffene Kundschaft davon Kenntnis erhält, die nicht aus erster Hand von der Information im Rahmen der öffentlichen Bekanntmachung erfährt. Inhaltlich wäre derselbe Informationsgehalt mitzuteilen wie im Rahmen einer individuellen Information. Nach dem Gesagten erweist sich eine öffentliche Bekanntmachung grundsätzlich als möglich.

E. 6.4

Nachfolgend bleibt zu prüfen, ob eine öffentliche Bekanntmachung verhältnismässig ist.

E. 6.4.1

Die Beschwerdeführerin macht geltend, eine öffentliche Bekanntmachung sei unverhältnismässig. Sie ist der Ansicht, diese wäre - wenn überhaupt - nicht ähnlich wirksam wie eine individuelle und direkte Meldung an einzelne betroffene Personen. Zudem würden fast alle Besucherinnen und Besucher der Internetseite durch die öffentliche Bekanntmachung erheblich und ohne Not verunsichert. Die öffentliche Bekanntmachung sei deshalb weder geeignet noch zumutbar.

E. 6.4.2

Die Verhältnismässigkeit ist ein verfassungsrechtlicher Grundsatz rechtsstaatlichen Handelns (Art. 5 Abs. 2 BV). Er umfasst nach Lehre und Rechtsprechung drei Elemente, die kumulativ beachtet werden müssen: Eine Massnahme muss geeignet und erforderlich sein, um ein im öffentlichen oder privaten Interesse liegendes Ziel zu verwirklichen, und sie muss zumutbar bleiben (vgl. BGE 147 I 346 E. 5.5). Es muss mit anderen Worten eine vernünftige Zweck-Mittel-Relation bestehen (vgl. bspw. BGE 148 II 392 E. 8.2).

E. 6.4.3

Vorliegend kann die von der Datenschutzverletzung betroffene Kundschaft nicht mehr identifiziert werden. Eine persönliche Benachrichtigung ist daher ausgeschlossen. Eine öffentliche Bekanntmachung stellt das einzige Mittel dar, um die betroffenen Personen erreichen zu können. Auch wenn damit nicht ausschliesslich tatsächlich von der Datenschutzverletzung Betroffene erreicht werden, ist die Massnahme dennoch geeignet, da sie der betroffenen und erreichten Kundschaft ermöglicht, entsprechende Schutzmassnahmen zu ergreifen. Auch dient diese Information der betroffenen Kundschaft, ihre allfälligen gesetzlichen Rechte im Zusammenhang mit der Datenschutzverletzung bei Dritten wahren zu können. Die unvermeidliche Folge, dass auch nicht von der Datenschutzverletzung betroffene Personen erreicht werden, vermag die Geeignetheit der Massnahme nicht in Frage zu stellen. Die öffentliche Bekanntmachung ist auch deshalb geeignet, weil die Beschwerdeführerin die Art der Mitteilung massgeblich bestimmen (Kommunikationskanal, begleitete Stellungnahme, getroffene Massnahmen, zu ergreifende Verbesserungsmassnahmen usw.) und so ausgestalten kann, dass sie sachlich, transparent (sekundärer Zweck der Informationspflicht) und lösungsorientiert wirkt.

E. 6.4.4

Eine Massnahme ist erforderlich, wenn der angestrebte Erfolg nicht durch gleich geeignete, aber mildere Massnahmen erreicht werden kann. Vorliegend steht keine andere Massnahme zur Verfügung, mit der die betroffenen Personen erreicht werden könnten. Denn selbst wenn die Information der einzelnen Kundschaft technisch möglich wäre, so würde dies einen unverhältnismässig hohen Aufwand verursachen; zudem wäre auch damit nicht

gewährleistet, dass Kundinnen und Kunden ohne Kundenkonto überhaupt noch ermittelt werden könnten. Die öffentliche Bekanntmachung erweist sich damit als das mildeste wirksame Mittel. Wie bereits dargelegt, gebietet der Verhältnismässigkeitsgrundsatz, die öffentliche Bekanntmachung einem vollständigen Verzicht auf eine Information vorzuziehen.

E. 6.4.5

Schliesslich ergibt sich die Zumutbarkeit einer Massnahme aus einer umfassenden Interessenabwägung zwischen privaten und öffentlichen Interessen. Dazu sind die Persönlichkeitsrechte der betroffenen Kundinnen und Kunden den Interessen der Beschwerdeführerin gegenüberzustellen. Auf Seiten der betroffenen Personen steht das Interesse, von der Datenschutzverletzung Kenntnis zu erhalten, um die geeigneten Schutzmassnahmen ergreifen zu können. Angesichts des bestehenden Schutzbedürfnisses kommt diesem Interesse erhebliches Gewicht zu. Demgegenüber steht das Interesse der Beschwerdeführerin nicht öffentlich zu informieren, um keinen Reputationsschaden zu erleiden und nicht betroffene oder potenzielle Kundschaft nicht unnötig zu verunsichern. Das Interesse am Schutz des geschäftlichen Rufs ist grundsätzlich anzuerkennen. Zu berücksichtigen ist jedoch, dass der allfällige Reputationsschaden seine Ursache in einer von der Beschwerdeführerin selbst zu verantwortenden Datenschutzverletzung hat. Es widerspräche dem Schutzzweck des Datenschutzrechts, wenn sich eine (juristische) Person unter Hinweis auf mögliche Reputationsschäden der Information der Betroffenen entziehen könnte. Dass auch nicht betroffene oder potenzielle Kundschaft Kenntnis von einer Datenschutzverletzung erlangt, stellt keine unverhältnismässige Zusatzbelastung dar, zumal die Mitteilung sachlich erfolgen und auf das Notwendige beschränkt werden kann. Insgesamt überwiegt das Interesse der betroffenen Person am Schutz ihrer Persönlichkeit das Interesse der Beschwerdeführerin an der Vermeidung einer öffentlichen Information; die Massnahme erweist sich demnach auch als zumutbar.

E. 6.4.6

Nach dem Gesagten ist die öffentliche Bekanntmachung als verhältnismässig zu qualifizieren.

E. 6.5

An die öffentliche Bekanntmachung stellt das Gesetz keine formalen Anforderungen. Sie kann beispielsweise erfolgen, indem der Verantwortliche die Information in gut sichtbarer Weise auf seiner Webseite publiziert (etwa durch den Einsatz eines prominent platzierten Banners) oder indem er einen entsprechenden Beitrag in einem Online-Forum veröffentlicht, sofern davon ausgegangen werden kann, dass die von der Verletzung der Datensicherheit betroffenen Personen die jeweilige Plattform regelmässig frequentieren. Denkbar sind sodann Mitteilungen in Medien, zum Beispiel Anzeigen in Tageszeitungen. Die öffentliche Bekanntmachung kann auch über mehrere Kanäle gleichzeitig beziehungsweise zusätzlich zur individuellen Information an einzelne betroffene Personen erfolgen. In inhaltlicher Hinsicht ist über dieselben Aspekte wie bei der individuellen Meldung zu orientieren, ansonsten die Information der betroffenen Person nicht «in vergleichbarer Weise» sichergestellt werden kann. In der Praxis dürfte eine öffentliche Bekanntmachung insbesondere dort in Betracht kommen, wo sich die konkret betroffenen Personen nicht eruieren lassen oder wo deren individuelle Information einen unverhältnismässigen Aufwand erfordern würde. Dem DSG lässt sich allerdings keine

(ausdrückliche) Pflicht entnehmen, in solchen Fällen eine öffentliche Bekanntmachung vorzunehmen (zum Ganzen vgl. Mathys/Thomann, in: Blechta/Vasella [Hrsg.], a.a.O. N. 94 und 95 zu Art. 24). Die Information muss mindestens Angaben zur Art der Verletzung, zu den Folgen für die betroffenen Personen (einschliesslich der Risiken) und zu den getroffenen bzw. vorgesehenen Massnahmen, um den Mangel zu beheben und die Folgen zu mindern, beinhalten; zudem sind der Name und die Kontaktdaten einer Ansprechperson anzugeben, die als Anlaufstelle für die Kommunikation mit der betroffenen Person fungiert. Die Meldung sollte sich insbesondere dazu äussern, welche Massnahmen die betroffene Person selbst ergreifen kann beziehungsweise muss, um den mit der Verletzung der Datensicherheit einhergehenden Folgen und Risiken zu begegnen (z. B. unverzügliche Passwortänderung oder Kreditkartensperre). Je nach den konkreten Umständen hat der Verantwortliche die betroffene Person ausserdem darüber zu orientieren, welche Kategorien von Personendaten von der Verletzung betroffen sind, so etwa dann, wenn diesbezüglich ein Missbrauchspotenzial besteht. Die Information ist adressatengerecht zu vermitteln. Dabei ist zu bedenken, dass einer durchschnittlichen betroffenen Person der Fachjargon hinsichtlich der bei einer Verletzung der Datensicherheit oftmals technisch geprägten Materie nicht geläufig sein dürfte. Art. 15 Abs. 3 DSV schreibt deshalb vor, dass der Verantwortliche die notwendigen Angaben «in einfacher und verständlicher Sprache» mitzuteilen hat. Für die betroffene Person muss insbesondere nachvollziehbar sein, welche Vorkehrungen sie zu ihrem Schutz treffen soll. Dabei bietet es sich in der Regel an, die Information in derselben Sprache auszugestalten, die auch im sonstigen Geschäftsverkehr mit der betroffenen Person verwendet wird. Hinsichtlich der Meldung an die betroffene Person bestehen keine Formvorschriften. Grundsätzlich empfiehlt es sich aber, die Information in einer in Text nachweisbaren Form vorzunehmen (zum Ganzen vgl. Mathys/Thomann, in: Blechta/Vasella [Hrsg.], a.a.O. N. 94 i.V.m. 74- 77 zu Art. 24).

E. 7

Zusammenfassend ist festzuhalten, dass weder eine unvollständige oder unrichtige Feststellung des Sachverhaltes noch eine Verletzung von Bundesrecht durch die Vorinstanz vorliegt. Die angefochtene Verfügung der Vorinstanz ist nicht zu beanstanden. Die Beschwerde erweist sich demnach als unbegründet, weshalb sie abzuweisen ist.

E. 8.1

Bei diesem Verfahrensausgang gilt die Beschwerdeführerin als unterliegend. Sie hat daher grundsätzlich die Verfahrenskosten zu tragen (Art. 63 Abs. 1 VwVG). Wurde jedoch der Anspruch auf rechtliches Gehör beziehungsweise die behördliche Begründungspflicht, wie vorliegend, verletzt (E. 3.4), ist diesem Umstand bei der Bestimmung der Kosten- und Entschädigungsfolgen grundsätzlich angemessen Rechnung zu tragen (vgl. Urteile des BGer 1C_123/2023 vom 14. Oktober 2024 E. 14.2 und 9C_39/2020 vom 9. Oktober 2020 E. 2.2; Urteil des BVGer A-3119/2024 vom 9. Februar 2026 E. 9.1 mit weiteren Hinweisen). Der Beschwerdeführerin sind daher die reduzierten Verfahrenskosten von Fr. 1'500.- aufzuerlegen. Dieser Betrag ist dem Kostenvorschuss von Fr. 2'000.- zu entnehmen. Der Restbetrag von Fr. 500.- wird der Beschwerdeführerin nach Eintritt der Rechtskraft dieses Urteils zurückerstattet.

E. 8.2.1

Ganz oder teilweise obsiegenden Parteien ist von Amtes wegen oder auf Begehren eine Entschädigung für die ihnen erwachsenen notwendigen Kosten zuzusprechen (Art. 64 Abs.

1 VwVG; Art. 7 Abs. 1 VGKE). Aus denselben Überlegungen zur verletzten Begründungspflicht (E. 8.1) ist der Beschwerdeführerin trotz ihres Unterliegens eine reduzierte Parteientschädigung zu Lasten der Vorinstanz zuzusprechen (vgl. Urteil des BVGer A- 3119/2024 vom 9. Februar 2026 E. 9.1 mit weiteren Hinweisen). Wird wie vorliegend keine Kostennote eingereicht, ist die Entschädigung aufgrund der Akten zu bestimmen (Art. 14 Abs. 2 VGKE). Unter Berücksichtigung der anwendbaren Bemessungsfaktoren, insbesondere des relevanten zeitlichen Aufwands und der Schwierigkeit der Sache (Art. 8 ff. VGKE; Urteil des BVGer A-2989/2018 vom 4. September 2019 E. 10.2.1), erweist sich eine reduzierte Entschädigung von pauschal Fr. 500.- als angemessen.

E. 8.2.2

Die Vorinstanz hat unabhängig vom Verfahrensausgang keinen Anspruch auf eine Parteientschädigung (vgl. Art. 7 Abs. 3 VGKE).