BVwG
Bundesverwaltungsgericht
Republik Österreich

Postadresse:
Erdbergstraße 192 – 196
1030 Wien
Tel: +43 1 601 49 – 0
Fax: + 43 1 711 23-889 15 41
E-Mail: einlaufstelle@bvwg.gv.at
www.bvwg.gv.at

E N T S C H E I D U N G S D A T U M

2 6 . 0 3 . 2 0 2 4

G E S C H Ä F T S Z A H L

W 1 3 7 2 2 4 1 6 3 0 - 1 / 4 8 E

Schriftliche Ausfertigung des am 21.12.2023 mündlich verkündeten Erkenntnisses

I M N A M E N D E R R E P U B L I K !

Das Bundesverwaltungsgericht erkennt durch den Richter Mag. Peter HAMMER als Vorsitzender und die fachkundigen Laienrichterinnen Mag. Ursula ILLIBAUER sowie Mag. Martina CHLESTIL als Beisitzerinnen über die Beschwerde der XXXX , vertreten durch HOSP, HEGEN & Partner Rechtsanwälte, gegen das Straferkenntnis der Datenschutzbehörde vom 17.02.2021, GZ: 2020-0.675.335 (D550.325), nach Durchführung einer mündlichen Verhandlung, zu Recht:

A)

I. Die Beschwerde wird gemäß § 28 Abs. 2 VwGVG iVm Art. 5 Abs. 1 lit f und Art. 32 iVm Art. 83 Abs. 4 lit a DSGVO mit der Maßgabe als unbegründet abgewiesen, dass die Geldstrafe gemäß § 30 DSG mit EUR 50.000 (fünfzigtausend) bestimmt wird.

II. Gemäß § 64 Abs. 1, 2 VStG hat die Beschwerdeführerin einen Beitrag zu den Kosten des Strafverfahrens in der Höhe von EUR 5.000 (fünftausend) zu leisten.

B)

Die Revision ist gemäß Art. 133 Abs. 4 B-VG zulässig.

Entscheidungsgründe:

I. Verfahrensgang:

1. Die XXXX (= Beschuldigte im Verwaltungsstrafverfahren vor der Datenschutzbehörde und Beschwerdeführerin vor dem Bundesverwaltungsgericht) ist ein konzessioniertes Kreditinstitut gemäß § 1 Bankwesengesetz (BWG).

Mit Eingabe vom 30.10.2019 an die Datenschutzbehörde (= belangte Behörde) teilte die Beschwerdeführerin gemäß ihrer Verpflichtung nach Art. 33 DSGVO eine Verletzung des Schutzes personenbezogener Daten mit. Dabei führte diese soweit verfahrensrelevant aus, dass aufgrund eines menschlichen Fehlers eine Einladung zum Weltspartag (per e-mail), welche im Anhang irrtümlich eine Excel-Liste mit Datensätzen von 5971 Kundinnen und Kunden zweier Filialen sowie deren Betreuern enthalten habe, an 234 Kundinnen und Kunden verschickt worden sei. Die Beschwerdeführerin habe umgehend reagiert und sowohl technische Maßnahmen zur Rückholung der versendeten Emails, als auch eine direkte Kontaktaufnahme mit den Emailempfängern veranlasst und diese aufgefordert die E-Mail zu löschen sowie dies zu bestätigen.

Mit Eingabe vom 29.10.2019 erhob (im Zusammenhang mit dem verfahrensgegenständlichen Vorfall) eine betroffene Bankkundin eine Datenschutzbeschwerde an die belangte Behörde. Diese behauptete eine Verletzung im Recht auf Geheimhaltung und brachte zusammengefasst vor, dass sie am 29.10.2019 von einer Filiale der Beschwerdeführerin eine E-Mail bekommen habe, in deren Anhang sich eine Excel-Liste mit sämtlichen Kundendaten der Filiale, befunden habe. Diese enthalte unter anderem Angaben zum Einkommen, Kontogruppe, Alter und Kontostand. Die Daten seien Kundenbezeichnungen zugeordnet, die wie folgt aufgebaut seien: [Nachname] + [Ersten zwei Buchstaben des Vornamens] + [Zahl]. Eine Zuordnung zu einer natürlichen Person sei eindeutig möglich.

Das Beschwerdeverfahren der betroffenen Bankkundin wurde mit einem der Beschwerde stattgebenden Bescheid der belangten Behörde erledigt.

2. Mit verfahrenseinleitender Maßnahme vom 05.05.2020 übermittelte die belangte Behörde, aufgrund ihrer Wahrnehmungen im Rahmen der Meldung der Beschwerdeführerin gemäß Art. 33 DSGVO und dem oben genannten Beschwerdeverfahren einer betroffenen Person eine Aufforderung zur Rechtfertigung, da der Verdacht bestehe, diese habe als

datenschutzrechtlich Verantwortliche, im Vorfeld des Vorfalls vom 29.10.2019, nicht die geeigneten technischen und organisatorischen Maßnahmen ergriffen, um ein angemessenes Schutzniveau der verarbeiteten personenbezogenen Daten zu gewährleisten. Dies betreffe Maßnahmen wie die Pseudonymisierung und Verschlüsselung personenbezogener Daten, eine dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung, die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall sicherzustellen, sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu implementieren. Dies insbesondere dadurch, dass die Beschwerdeführerin die verfahrensgegenständliche „Excel-Datei“ in vollem Umfang, für einen uneingeschränkten Benutzerkreis unverschlüsselt und auch sonst ungeschützt über die IT-Netzwerkstruktur des Unternehmens verfügbar gehalten habe.

Es bestehe daher der Verdacht, dass die Beschwerdeführerin, auf die oben beschriebene Art und Weise, im Zusammenhang mit der gegenständlichen Datenverarbeitung, sowohl gegen den von Art. 5 Abs. 1 lit. f DSGVO normierten Grundsatz, als auch gegen die in Art. 32 DSGVO normierten Pflichten in Bezug auf die Sicherheit der Datenverarbeitung, in Form geeigneter technischer und organisatorischer Maßnahmen, zumindest unter Außerachtlassung der gebotenen Sorgfalt verstoßen habe.

3. Mit Rechtfertigung vom 18.06.2020 brachte die Beschwerdeführerin zusammengefasst vor, dass keine Verwaltungsübertretung vorliege bzw. sei – selbst bei Vorliegen einer Verwaltungsübertretung - eine Bestrafung nicht zulässig. Für die der Mitarbeiterin übertragene Aufgabe (Versendung von Einladungen zum Weltspartag) sei ein Vollzugriff auf die „Excel-Liste/Datei“ zwingend notwendig gewesen und habe die Filialleiterin die verfahrensgegenständliche Liste nur wenigen Mitarbeitern zur Erfüllung dieser speziellen Aufgabe ausgehändigt. Es fehle bereits an einer Identifizierbarkeit der in der Excel-Liste erfassten Personen durch die E-Mailempfänger bzw. sei ohne weitere Erläuterungen die Liste aufgrund der verwendeten Abkürzungen für einen Dritten unverständlich. Bereits vor dem gegenständlichen Vorfall habe ein geeignetes Netz an technischen und organisatorischen Maßnahmen bestanden, um ein angemessenes Schutzniveau zu gewährleisten. Alle EDV- und Datensicherheitssysteme seien auf dem aktuellen Stand der Technik und stelle dieses im Rahmen einer Abwägung der Implementierungskosten und der Eintrittswahrscheinlichkeit ein angemessenes Schutzniveau dar. Für die Verhängung einer Strafe über die Beschwerdeführerin sei Art. 5 Abs. 1 lit f DSGVO nicht konkret genug und stelle eine

Bestrafung wegen Art. 32 DSGVO und Art. 5 Abs. 1 lit f DSGVO einen Verstoß gegen das Doppelbestrafungsverbot dar. Darüber hinaus widerspreche die österreichische Rechtslage einer unmittelbaren Strafbarkeit einer juristischen Person und wäre im Fall einer Strafbarkeit mit einer Verwarnung oder Beratung gemäß Art. 58 DSGVO bzw. § 33a VStG vorzugehen. Aus diesen Gründen sei das gegenständliche Verwaltungsstrafverfahren einzustellen.

4. Mit Aufforderung zur Rechtfertigung vom 23.06.2020 an die Beschwerdeführerin weitete die belangte Behörde den Tatvorwurf, im Lichte der Entscheidung des Verwaltungsgerichtshofes vom 12.05.2020, Ro 2019/04/0229, dahingehend aus, dass der Verdacht bestehe, zwei Vorstandsmitglieder der Beschwerdeführerin seien gemeinsam oder als Teil des vertretungsbefugten Organs im Sinne der § 30 Abs. 1 und 2 DSG und § 9 Abs. 1 VStG, zumindest durch Außerachtlassung der gebotenen Sorgfalt, auf Grund mangelnder Kontrolle und Überwachung für die Verletzung von Art. 5 Abs. 1 lit f DSGVO und Art. 32 DSGVO verantwortlich. Die Strafbarkeit juristischer Personen wegen Verstößen gegen die DSGVO ergebe sich aus dem tatbestandsmäßigen, rechtswidrigen und schuldhaften Verhaltens einer Führungsperson gemäß § 30 Abs. 1 DSG.

5. Mit Rechtfertigung vom 23.07.2020 brachten (nunmehr) die konkreten Beschuldigten (= die Beschwerdeführerin und zwei Vorstandsmitglieder) gemeinschaftlich und ergänzend zur Rechtfertigung vom 18.06.2020 soweit wesentlich vor, dass eine zentrale Speicherung der Kundendaten bereits aufgrund der allgemeinen gesetzlichen Verpflichtungen für Kreditinstitute erforderlich sei. Der Zugriff auf diese Daten sei je nach Mitarbeiter auf die notwendigsten Abfragen bzw. Berechtigungen eingeschränkt. Eine systematische Auswertung könne nur durch eine spezielle Software, welche ausschließlich ausgewählten Mitarbeitern des Bereichs „Marktfolge“ zur Verfügung stehe, erfolgen. Diese Funktion sei zur Erfüllung von gesetzlichen Verpflichtung (z.B. § 1 Abs. 2 WiEReG nach § 6 FM-GwG), Controllingzwecken, zur Vertriebssteuerung und der Erhaltung der Datenqualität notwendig. Aus diesem Grund werde, wenn eine Arbeitsaufgabe dies erfordere, eine Excel-Liste durch einen Mitarbeiter der „Marktfolge“ generiert, diese auf den notwendigsten Kundenkreis eingeschränkt, und anschließend der jeweiligen Filiale übermittelt. Darüber hinaus sei der korrekte Umgang mit dieser Excel-Liste durch Arbeitsanweisungen abgesichert. Die dem Verfahren zugrundeliegende Datenschutzverletzung sei auf eine unabhängige Fehlleistung zweier Filialmitarbeiterinnen zurückzuführen. Insbesondere habe keine Berechtigung zum Versenden von Massenmails bestanden bzw. sei dies bereits durch eine Arbeitsanweisung untersagt. Dieses Fehlverhalten könne den von der belangten Behörde herangezogenen Vorstandsmitgliedern nicht als schuldhaftes Verhalten angelastet werden.

6. Die belangte Behörde lud den Abteilungsleiter für Finanzen und die unmittelbar betroffene Filialleiterin für 10.09.2020 zur Einvernahme als Zeugen vor Die Filialleiterin gab an, sie wisse nun über die Unzulässigkeit von „Massenmails“ auf Filialebene Bescheid, jedoch sei ihr dies zum Zeitpunkt des gegenständlichen Vorfalls nicht bewusst gewesen. Die Intention der Weisung zur Versendung der Einladungen sei der bevorstehende Weltspartag gewesen. Die Excel-Liste mit den Kundendaten sei auf dem Filiallaufwerk für die Mitarbeiter der Filiale bereitgestellt gewesen. Sowohl den Text des E-Mails, als auch die zu adressierenden Kunden habe sie als Filialleiterin vorab festgelegt. Nachdem die fehlerhafte Übermittlung aufgefallen war, habe ein Kollege sofort mit dem Rückruf der E-Mails begonnen, jedoch seien insgesamt 227 E-Mails unwiderruflich zugestellt worden. Der „Datenschutzbeauftragte der Beschwerdeführerin“ habe daraufhin angeordnet, dass ein zweites E-Mail an alle Empfänger ergehe und um die Löschung des gegenständlichen Emails mit einer zusätzlichen Bestätigung ersucht werde. Im Anschluss habe eine „Databreach-Notification“ an die belangte Behörde stattgefunden. Die in Frage stehende Mitarbeiterin sei absolut zuverlässig, es handle sich um einen Flüchtigkeitsfehler. Die Excel-Datei sei vorübergehend nicht mehr zur Verfügung gestanden und seien im Rahmen einer internen Überarbeitung die Kundennamen durch Kennungen ersetzt und E-Mailadressen entfernt worden. Zum Thema Datenschutz müsse alle zwei Jahre eine Schulung absolviert werden. Alle Kunden hätten teilweise per E-Mail, teilweise per Telefon die Löschung der verfahrensgegenständlichen E-Mails bestätigt.

Der Abteilungsleiter für Finanzen erklärte, die Excel-Datei werde aus einer zentralen Datenbank erstellt. Die Datei stamme aus dem Bereich „Marktfolge“ und werde dort von berechtigten Person im erforderlichen Umfang erstellt. Innerhalb einer Excel-Datei werde immer nur der Datensatz einer bestimmten Filiale dargestellt. So auch im Falle der versendeten Excel-Liste vom 29.10.2019. Anhand der Datei erkenne der Filialleiter etwa die Anzahl der jeweiligen Kunden eines einzelnen Mitarbeiters sowie die entsprechenden Kerndaten. Die Existenz dieser Datei sei dem Vorstand bekannt. Technisch gesehen gelange die Datei durch einen automatisierten Vorgang auf den Filialordner innerhalb der Firmennetzwerkinfrastruktur (geschützter Bereich) und sei sodann für die Filialleitung und die zuständigen Filialmitarbeiter verfügbar. Der Versand der fehlerhaften Massenmails sei durch eine Fehlentscheidung der Filialleiterin ins Rollen gekommen, da diese sich für derartige Aussendungen an den Bereich Geschäftsintensivierung und Prozessmanagement wenden hätte müssen. Die dafür erlassene Arbeitsanweisung sei im Unternehmensnetzwerk frei abrufbar und würden diese jährlich im Rahmen einer Schulung verfestigt. Einen Passwortschutz habe die Excel-Datei nicht, da diese ohnehin im internen Firmennetzwerk gesichert und nur den jeweiligen Filialmitarbeitern zugänglich sei.

7. Mit ergänzender Rechtfertigung vom 15.10.2020 nahmen die Beschuldigten zu den Zeugeneinvernahmen vom 10.09.2020 Stellung und führten wiederholend und soweit verfahrensrelevant aus: Die Filialleiterin sei aufgrund der gültigen Arbeitsanweisungen und der jährlich stattfindenden Schulung im Umgang mit elektronischen Medien in Kenntnis des Verbotes des Versands von Massenemails gewesen. Auch würden E-Mails über den internen Nachrichtendienst das Wissen über die einzuhaltende Emailkultur regelmäßig auffrischen. Zum Zeitpunkt des Inkrafttretens der DSGVO (2018) habe eine datenschutzspezifische Schulung stattgefunden.

8. Für 16.11.2020 lud die belangte Behörde jene Angestellte, welche die Emails mit dem irrtümlichen Anhang versendete, als Zeugin im Verwaltungsstrafverfahren vor. Die Zeugin führte soweit verfahrensrelevant und zusammengefasst aus: Ihr sei eine Arbeitsanweisung betreffend Massenemails zwar grundsätzlich bekannt, habe jedoch die Entscheidung ihrer Führungskraft (Filialleiterin) nicht in Frage gestellt. Der betreffende Monat sei besonders stressig gewesen und habe sie um Zeit zu sparen die „Weiterleitungsfunktion“ über die versendete E-Mail ihrer Vorgesetzten genutzt. Dabei habe sie vergessen die Excel-Liste aus dem Anhang zu löschen. Sie könne sich den Fehler nur durch eine Unaufmerksamkeit erklären. Aktuell könne nur über die Genehmigung der Vorgesetzten auf eine pseudonymisierte Version der ursprünglichen Liste zugegriffen werden. Es habe 2018 eine Datenschutzschulung stattgefunden, welche all zwei Jahre aufgefrischt werde. Darin sei jedoch kein Hinweis auf Massenmails enthalten gewesen.

9. Mit ergänzender Rechtfertigung vom 03.12.2020 führten die Beschuldigten aus, beide Zeugen hätten bestätigt, dass regelmäßig eine Schulung zu datenschutzrelevante Themen durchgeführt werde und entsprechende Arbeitsanweisungen implementiert seien. Es liege keinesfalls Organisationsverschulden vor.

10. Die beiden Vorstandsmitglieder, welche für die Ressorts „Markt“ und „Marktfolge“ zuständig sind, führten bei einer Befragung am 27.01.2021 soweit wesentlich und verfahrensrelevant aus, dass die Liste bereits seit einem sehr langen Zeitraum im Unternehmen existiere und keine genauen Aussagen zu deren Ursprung getroffen werden könne. Die Verwendung resultiere aus den notwendigen Arbeitsabläufen, welche systemische Daten vorauszusetze. Im Unternehmen habe es ein großes Schulungsprogramm für alle Mitarbeiter zum Thema Datenschutz im Zuge des Inkrafttretens der DSGVO gegeben. Ein Arbeiten ohne diese Datei oder in reduzierter Form stelle ein großes Hindernis für den täglichen Arbeitsablauf dar. Niemand habe Probleme oder Bedenken datenschutzrechtlicher Natur an den Vorstand herangetragen und könne ein menschlicher Fehler nie vollkommen

ausgeschlossen werden. Auch hätte es keine Empfehlungen zu weiteren Schutzmaßnahmen gegeben.

11. Mit 17.02.2021 erließ die belangte Behörde das angefochtene Straferkenntnis gegen die Beschwerdeführerin wegen der Verletzung ihrer Pflicht zur Einhaltung des Verarbeitungsgrundsatzes der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 lit f DSGVO sowie die Verletzung der in Art. 32 DSGVO normierten Pflichten hinsichtlich der Sicherheit der Datenverarbeitung in Form geeigneter technischer und organisatorischer Maßnahmen. Ihr sei das rechtswidrige und schuldhafte Verhalten zweier Vorstandmitglieder, welche zur Vertretung nach außen berufenen seien, zuzurechnen. Die verhängte Strafe betrug EUR 4.000.000, woraus sich ein Kostenbeitrag von EUR 400.000 ergab.

Dabei führte die DSB rechtlich aus, dass die verfahrensgegenständliche Excel-Liste personenbezogene Daten enthalte. Ein Kundenkürzel ändere daran nichts. Auch der Frage, ob die Datei geöffnet worden sei, komme in diesem Zusammenhang keine Relevanz zu. Die Übermittlung der E-Mails stelle eine Verarbeitung gemäß Art. 4 Z 2 DSGVO dar. Das festgestellte Verhalten der Beschwerdeführerin weiche von den einschlägigen Bestimmungen der DSGVO sowie den Anforderungen des Art. 32 Abs. 1 DSGVO in mehrfacher Hinsicht ab. Im vorliegenden Fall habe keines der beiden Vorstandsmitglieder und auch nicht der Datenschutzbeauftragte, das mittlere Management oder die Mitarbeiter auf Filialebene die technische Ausgestaltung sowie den Inhalt und Umfang der versehentlich nach außen gelangten Excel-Datei als datenschutzrechtlich kritisch oder problematisch angesehen. Auch habe weder die betroffene Filialleiterin, noch der Großteil der als Zeugen befragten Filialmitarbeiter die unternehmensinterne Arbeitsanweisung, wonach das Versenden von Massenmailings untersagt sei, gekannt. Dies zeuge jedenfalls nicht vom Bestehen einer dem Risiko angemessenen und allen Bediensteten bekannten IT-Strategie sowie von am Stand der Technik orientierten technischen und organisatorischen Maßnahmen. Eine Risikoanalyse, Evaluierung und Verschlüsslung der genannten Excel-Liste/Datei stehe auch nicht im Konflikt mit der Berücksichtigung der Implementierungskosten oder den Umständen der Datenverarbeitung.

Die zu bestimmende Eintrittswahrscheinlichkeit einer datenschutzrechtlichen Problematik sei als „Hoch“ einzustufen, da es sich um eine Verarbeitung von bankspezifischen Kundendaten im Wege einer völlig ungeschützten Excel-Datei auf Filialebene handle. Die Vorgaben des Art. 5 Abs. 1 lit f und Art. 32 DSGVO seien daher nicht eingehalten worden. Das Verhalten der Vorstandsmitglieder sei der Beschwerdeführerin zuzurechnen, diese hätten kein wirksames Kontrollsystem zur Einhaltung der datenschutzrelevanten Bestimmungen etabliert. Im

Rahmen der Strafbemessung sei mangels eindeutiger gesetzlicher Bestimmungen die Strafe vom Jahresumsatz des Mutterkonzerns (und nicht allein von jenem der Beschwerdeführerin) zu bemessen. Daraus ergebe sich eine Berechnungsbasis in Höhe von 6.188.900.000 EUR. Erschwerend sei die Art, Schwere und Dauer des Verstoßes, die Wiedereinführung der Excel-Datei in (lediglich) leicht modifizierter Form und die grobe Fahrlässigkeit der Vorstandsmitglieder zu werten; mildernd sei das erstmalige verwaltungsstrafrechtliche Aufscheinen und die Kooperation im Ermittlungsverfahren zu berücksichtigen.

12. Gegen das genannte Straferkenntnis richtet sich verfahrensgegenständliche Beschwerde vom 17.03.2021. Diese brachte zusammengefasst vor, die belangte Behörde habe zu Unrecht eine wirtschaftliche Einheit der Beschwerdeführerin mit der zugehörigen Muttergesellschaft XXXX angenommen und unabhängig davon eine unrichtige Bemessungsgrundlage herangezogen. Die Wiederverwendung der identen Excel-Liste in der gleichen Art und Weise sei ebenso unrichtig festgestellt worden wie ein Fehlen von internen und externen Überprüfungen der technischen Ausgestaltung der Excel-Datei. Zudem sei eine bereits eingetretene Verfolgungsverjährung missachtet worden und verstoße das Straferkenntnis gegen § 44a Z 1 VStG. Der Begriff der Integrität sei unrichtig beurteilt worden und die § 11 DSG und § 33a VStG unangewendet geblieben.

Aus den unrichtigen Feststellungen würden sich darüber hinaus zahlreiche sekundäre Feststellungsmängel sowie eine unrichtige rechtliche Beurteilung ergeben. Zudem habe die belangte Behörde das Parteiengehör der Beschwerdeführerin verletzt, keine Erhebungen zum ausschlaggebenden Geschäftsjahr durchgeführt und es mangle es an einer Erhebung oder Zuordenbarkeit der Daten. Auch sei das verfassungsgesetzlich verankerte Bestimmtheitsgebot durch Art. 5 Abs. 1 lit f DSGVO nicht erfüllt. Schließlich hinaus habe die belangte Behörde eine fehlerhafte Strafbemessung durchgeführt.

13. Mit Schreiben vom 15.04.2021 legte die belangte Behörde die Beschwerde samt dem zugehörigen Verwaltungsakt dem Bundesverwaltungsgericht vor, beantragte die Abweisung der Beschwerde, verwies vollinhaltlich auf das bekämpfte Erkenntnis und führte zur Bescheidbeschwerde der Beschwerdeführerin ergänzend aus, dass keine Verletzung des Rechts auf ein faires Verfahren vorliege, da die Durchführung einer mündlichen Verhandlung im Ermessen der Behörde stehe und kein abstraktes Recht des Beschuldigten oder seines Rechtsanwaltes existiere, an der Vernehmung der Zeugen teilzunehmen und diese zu befragen. Auch stimme die Behauptung der Unrichtigkeit, betreffend die Feststellung der „Wiederverwendung“ einer leicht modifizierten Excel-Datei, nicht, da trotz Änderung des Kundenkürzels und Entfernung der E-Mailadressen im Falle einer erneuten Offenlegung durch

unberechtigte Dritte mit relativ einfachen Mitteln aufgrund des Umfangs der enthaltenen Daten (Einkommens- und Vermögenskennzahlen, Adressbestandteile, Zuordnung zu einer bestimmten Bankfiliale als Kundin oder Kunde) Rückschlüsse auf eine identifizierbare Person hergestellt werden könnten. Die herangezogene Bemessungsgrundlage sei nach Ansicht der belangten Behörde korrekt ermittelt worden, da es keine gesetzlichen und in den Erwägungsgründen ersichtliche Anhaltspunkte für deren genauen Bestimmung gebe.

14. Mit ergänzenden Stellungnahmen regte die belangte Behörde die Aussetzung des gegenständlichen Beschwerdeverfahrens an, da beim EuGH (C-807/21) ein Vorabentscheidungsersuchen zu der Frage anhängig sei, ob eine juristische Person unmittelbar Betroffene im Bußgeldverfahren wegen eines Verstoßes gegen Art. 83 DSGVO sein könne.

15. Mit Beschluss des Bundesverwaltungsgerichtes vom 18.05.2022 wurde das Verfahren hinsichtlich des beim EuGH anhängigen Verfahrens zu C-807/21 ausgesetzt. Dieser Beschluss erwuchs mangels Anfechtung in Rechtskraft.

16. Mit Schreiben vom 03.05.2023 informierte das Bundesverwaltungsgericht die Verfahrensparteien des gegenständlichen Strafverfahrens über den ergangenen Schlussantrag in der Rechtssache C-807/21 sowie die Zulässigkeit von Ermittlungsschritten während eines ausgesetzten Verfahrens. Unter einem wurden die Verfahrensparteien um Stellungnahmen ersucht und Verhandlungstermine (während des ausgesetzten Verfahrens) ab Juni 2023 in Aussicht gestellt.

Die DSB teilte am 12.05.2023 mit, dass die vorgesehene Entscheidung – so sie dem Schlussantrag folge – für eine maßgebliche Veränderung der Rechtslage sorgen könne, da die bisherige Judikatur des Verwaltungsgerichtshofes zur Strafbarkeit der juristischen Person nicht mehr aufrecht zu erhalten sei. Die Bemessungsgrundlage für die zu verhängende Strafe sei im Rahmen der „wirtschaftlichen Einheit“ zu beurteilen, dies treffe auf eine einhundertprozentige Tochter einer Muttergesellschaft zu.

Mit Stellungnahme vom 16.05.2023 führte die Beschwerdeführerin aus, dass § 38a AVG nicht zur Setzung von Verfahrensschritten herangezogen werden könne, da das Bundesverwaltungsgericht dem EuGH keine eigenständige Frage zur Vorabentscheidung vorgelegt habe. Es handle sich um eine Aussetzung gemäß § 17 VwGVG iVm § 38 AVG bis zum Vorliegen einer Vorabentscheidung des EuGH. § 38 AVG erlaube keine Setzung von Ermittlungsschritten während eines ausgesetzten Beschwerdeverfahrens und führe eine faktische Fortsetzung des Verfahrens zum Weiterlaufen der Entscheidungs- und

Verjährungsfristen. Verwiesen wurde insbesondere auch auf §§ 163 und 190 ZPO, die in diesem Kontext vergleichbar seien. Den Interpretationen der Behörde zum Schlussantrag des Generalanwalts zur Rechtssache C-807/21 sei nicht zu folgen. Darüber hinaus stellte die Beschwerdeführerin fünf Beweisanträge, unter anderem die Einholung eines Sachverständigengutachtens aus dem Bereich IT-Sicherheit und eines Buchsachverständigengutachtens.

17. Das Bundesverwaltungsgericht beraumte am 17.05.2023 eine mündliche Verhandlung für den 07.06.2023 – ausdrücklich zum Thema der Berechnungsgrundlage für die Strafe – an. Vorbereitend führte die Beschwerdeführerin aus, die Behörde haben den Umsatz mit der Bilanzsumme verwechselt. Zudem sei nur jener Umsatz der konkreten Aktiengesellschaft und nicht jener der Muttergesellschaft heranzuziehen, zumal nie gegen die Muttergesellschaft ermittelt worden sei. Insofern sei eine Verfolgungsverjährung gemäß § 31 VStG eingetreten. Bei einer Strafe gegen die Beschwerdeführerin wäre ein Umsatz von 146,6 Millionen Euro heranzuziehen gewesen.

18. Am 07.06.2023 fand am Bundesverwaltungsgericht eine öffentliche mündliche Verhandlung statt, an welcher die Beschwerdeführerin, deren Rechtsvertretung und ein Vertreter der belangten Behörde teilnahmen. Dabei wandte sich die Datenschutzbehörde – im Sinne der übermittelten Rechtsansicht des Bundesverwaltungsgerichts – einerseits gegen die Argumentation der Beschwerdeführerin im Zusammenhang mit § 38a AVG, andererseits gegen mehrere der Beweisanträge. Für die Strafbemessung sei der Jahresumsatz des Konzerns heranzuziehen. Zur Ladung von Zeugen wurde die Verhandlung auf 04.07.2023 vertagt. Die Ladungen wurden am 15.06.2023 abgefertigt.

19. Mit Schreiben vom 26.06.2023 ersuchte der Generaldirektor der Beschwerdeführerin um Vertagung seiner Befragung aufgrund eines Urlaubs. Mit Schreiben vom 27.06.2023 ersuchte der Vorstandsdirektor der Beschwerdeführerin um Vertagung der Befragung aufgrund einer wichtigen (nicht verschiebbaren) Sitzung. Ebenfalls mit Schreiben vom 27.06.2014 ersuchte der Leiter der Personalabteilung um Vertagung seiner Befragung aufgrund nicht delegierbarer dienstlicher Verpflichtungen.

In Reaktion darauf schrieb das Bundesverwaltungsgericht weitere Verhandlungstermine am 26.07.2023 sowie 07.08.2023 aus und lud dazu die oben angeführten Zeugen. Mit Schreiben vom 30.06.2023 wurden die Verfahrensparteien informiert, dass die anberaumte Verhandlung am 04.07.2023 jedenfalls zur Befragung von zwei weiteren geladenen Zeugen stattfinden werde. Ergänzend wurde nochmals darauf hingewiesen, dass das Verfahren

weiterhin ausgesetzt sei, weil die Verhandlungen den Sachverhalt, nicht aber die Rechtsfrage in der Rechtssache C-807/21 des EuGH klären sollen.

20. Am 04.07.2023 setzte das Bundesverwaltungsgericht die öffentliche und mündliche Verhandlung fort. Der verantwortliche Beauftragte gab befragt an, dass er nicht wisse, warum er in das gegenständlichen Verwaltungsstrafverfahren nicht eingebunden worden sei; es habe jährliche Datenschutzschulungen gegeben und es bestehe eine Dienstanweisung zum Verbot von Versand von Massenmails, wobei eine genaue Definition, ab wann „Masse“ vorliege, nicht vorliege. Eine diesbezügliche Zuständigkeit liege in der Abteilung für Geschäftsintensivierung und Prozessmanagement. Alle Empfänger des E-Mails (mit dem irrtümlichen Anhang) hätten die Löschung bestätigt. Die versendete Excel-Liste sei nicht selbsterklärend und habe sogar die Datenschutzbehörde eine Erläuterung der Bezeichnungen verlangt. Die Erläuterung sei nicht mit den verfahrensgegenständlichen E-Mails übermittelt worden. Andere Banken hätten ähnliche System und Arbeitsaufläufe für ihre Filialen implementiert. Die aktuell in Verwendung stehende Excel-Liste sei überarbeitet und nunmehr vollständig pseudonymisiert.

Die Leiter des Bereichs für Finanzen (ehemals Geschäftsintensivierung und Prozessmanagement) gab befragt an, dass ungefähr 5 bis 10 Massenmails im Jahr 2019 durchgeführt worden seien und die Filiale die dafür zuständige Abteilung kontaktieren müsse. Das Betriebsergebnis der Beschwerdeführerin belaufe sich auf EUR 146,6 Millionen. Das Controlling erstelle die Excel-Datei im erforderlichen Umfang und sei der Ordner, in welchem sich die Excel-Liste in den Filialen befinde, mit einem Passwort geschützt. Verstöße habe es in diesem Zusammenhang soweit bekannt nie gegeben.

21. Am 21.07.2023 setzte das Bundesverwaltungsgericht die öffentliche mündliche Verhandlung fort. Die Aussage des Vorstands für das Ressort „Marktfolge“ wurde hinsichtlich der bereits getätigten Ausführungen ausschließlich konkretisiert bzw. verwies dieser auf seine bisherigen Aussagen im Verwaltungsstrafverfahren.

Der Leiter der Personalabteilung der Beschwerdeführerin gab befragt an, dass dieser mit der Koordinierung der Datenschutzschulungen befasst sei und die entsprechenden Nachweise administriere bzw. im Schadensfall diese den internen Gremien vorlege. Persönliche Wahrnehmungen über eine Schulung betreffend Versand von Massenmails habe er nicht.

22. Mit Stellungnahme vom 21.08.2023 wies die belangte Behörde auf ein weiteres anhängiges Vorabentscheidungsverfahren (C-383/23) hin, welches zur Beurteilung der gegenständlichen Rechtsfragen aus ihrer Sicht relevant sei.

23. Am 22.09.2023 setzte das Bundesverwaltungsgericht die öffentliche mündliche Verhandlung fort. Das Vorstandsmitglied für das Ressort „Markt“ gab befragt soweit verfahrensrelevant an: Alle Empfänger der unabsichtlich übermittelten Excel-Liste seien umgehend informiert worden und sei eine Löschung bestätigt worden. Aus der aktuellen Excel-Datei, welche seit Februar 2020 verwendet werde, sei kein Rückschluss mehr auf natürliche Personen möglich und seien die kompromittierten Datensätze nach ihrer Recherche bislang nicht im Internet oder Darknet aufgetaucht.

Die belangte Behörde führte ergänzend aus, dass der EuGH in diesem Zusammenhang in einer rezenten Entscheidung klargestellt habe, dass der Verantwortliche in Bezug auf eine Verarbeitung personenbezogener Daten die Beweislast für die Einhaltung der Grundsätze nach Art. 5 Abs. 1 DSGVO trage. Zudem gehe ein vorgebrachter Verfahrensfehler, hinsichtlich des ausgesetzten Verfahrens, ins Leere, da dieses mit gesondert anfechtbaren Beschluss ausgesetzt worden sei.

24. Mit Verständigung vom 06.12.2023 informierte das Bundesverwaltungsgericht über die ex lege Beendigung der Aussetzung des gegenständlichen Beschwerdeverfahrens, da der EuGH in der Rechtssache C-807-21 ein Urteil erlassen habe. Art. 58 Abs. 2 Buchst. i und Art. 83 Abs. 1 bis 6 DSGVO seien dahingehend auszulegen, dass sie einer nationalen Regelung entgegenstehen, wonach eine Geldbuße wegen eines in Art. 83 Abs. 4 bis 6 DSGVO genannten Verstoßes gegen eine juristische Person in ihrer Eigenschaft als Verantwortliche nur dann verhängt werden könne, wenn dieser Verstoß zuvor einer identifizierten natürlichen Person zuzurechnen sei. Art. 83 DSGVO sei dahin auszulegen, dass nach dieser Bestimmung eine Geldbuße nur dann verhängt werden dürfe, wenn nachgewiesen sei, dass der Verantwortliche, der eine juristische Person und zugleich ein Unternehmen sei, einen in Art. 83 Abs. 4 bis 6 DSGVO genannten Verstoß vorsätzlich oder fahrlässig begangen habe.

Die Aussetzung des Verfahrens sei mit der oben angeführten EuGH-Entscheidung ex lege beendet.

Bereits zuvor war die Fortsetzung der Verhandlung für 21.12.2023 anberaumt worden.

25. Die Verfahrensparteien brachten jeweils eine weitere Stellungnahme vom 18.12.2023 und 19.12.2023 beim Bundesverwaltungsgericht ein wobei die Ausführungen des EuGH teils diametral interpretiert wurden.

26. Mit Beschluss des Bundesverwaltungsgerichtes vom 19.12.2023 wurden die Beweisanträge der Beschwerdeführerin auf Einholung eines Sachverständigengutachtens aus

dem Bereich IT-Sicherheit und die Einholung eines Buchsachverständigengutachtens abgewiesen. Diese sein zur Beurteilung der gegenständlichen Sachverhaltsfragen nicht erforderlich.

27. Am 21.12.2023 setzte das Bundesverwaltungsgericht die öffentliche mündliche Verhandlung fort, an welcher die Beschwerdeführerin, deren Rechtsvertretung und ein Vertreter belangten Behörde teilnahmen. Dabei wurde den Verfahrensparteien bekannt gegeben, dass sich der Senat bei der allfälligen Strafbemessung an den Leitlinien 04/2022 für die Berechnung von Geldbußen im Sinne der DSGVO des Europäischen Datenschutzausschusses, Version 2.1; angenommen am 24. Mai 2023 (auch „Guidelines“ des EDPB) orientieren werde.

Nach Erörterung der verfahrensrelevanten Rechtsfragen der Abweisung der bisher nicht erledigten Beweisanträge, hinsichtlich der namentlich genannten Zeugen vom 18.12.2023 und 21.12.2023, mit verfahrensleitendem Beschluss und der abschließenden Vorträge der Verfahrensparteien verkündete der erkennende Richter nach Durchführung der nichtöffentlichen Beratung des Senates gemäß § 29 Abs. 2 VwGVG das Erkenntnis samt den wesentlichen Entscheidungsgründen und erteilte die Rechtsmittelbelehrung.

Nach Verkündung des Erkenntnisses beantragten die Beschwerdeführerin und die belangte Behörde eine schriftliche Ausfertigung der Entscheidung.

II. Das Bundesverwaltungsgericht hat erwogen:

1. Feststellungen:

1.1. Die Beschwerdeführerin ist ein im Firmenbuch eingetragenes konzessioniertes Kreditinstitut gemäß § 1 Bankwesengesetz (BWG). Diese weist im Geschäftsjahr 2019 einen Betriebsertrag/Umsatz in der Höhe von EUR 146.618.626,52 aus und eine Bilanzsumme von EUR 6.155.416.429,72.

1.2. Die Beschwerdeführerin betreibt ein eigenständiges Bankfilialennetzwerk und ist eine (beinahe) einhundertprozentige Tochter ihrer Muttergesellschaft „ XXXX “. Sie tritt eigenständig am Markt auf und handelt selbstbestimmt. Der Datenschutzbeauftragte des Mutterkonzerns ist auch für die Tochtergesellschaften zuständig bzw bestellt worden. Diese wiederum verfügen über eigenständige Verantwortliche Beauftragte iSd § 9 Abs 2 VStG auf Fillialebene, mitunter auch für den Themenkomplex „Datenschutz“. Der Konzern-Datenschutzbeauftragte wurde seitens der DSB im gegenständlichen Verfahren nicht eingebunden.

1.3. Die Filialleiterin hat im Vorfeld des Vorfalles vom 29.10.2019 die in der Filiale tätigen Kundenbetreuer angewiesen, mittels E-Mail, die jeweils von ihnen betreuten Kunden zum Weltspartag einzuladen. Die Filialleiterin hatte im Vorfeld in der Excel-Datei entsprechende Auswahl-Filter gesetzt, sodass den einzelnen KundenbetreuerInnen bereits die Auswahl der von ihnen betreuten bzw. einzuladenden Kunden dargestellt wurde (Excel-Listen). Die derart gefilterte Liste wurde dann von der Filialleiterin den jeweiligen KundenbetreuerInnen per E-Mail, mit dem Auftrag der Einladung der ausgewählten Kunden, zugeschickt. Den Text der E-Mailnachricht hat die Filialleiterin selbst vorgegeben und die Weisung erteilt die E-Mailadressen der Empfänger in das Feld BCC des E-Mailprogramms einzufügen.

1.4. Die gegenständliche Datei enthielt neben den E-Mail-Adressen noch weitere Kundendaten, die aufgrund eines vergleichsweise simpel zu identifizierenden Personenkürzels – [Nachname] + [Ersten zwei Buchstaben des Vornamens] + [Zahl] – ohne großen Aufwand mit konkreten Kunden in Verbindung gebracht werden konnten. Eine zusätzliche Sicherung, etwa in Form einer weitergehenden Verschlüsselung der Datei selbst, bestand nicht.

1.5. Die Versendung von 234 E-Mailnachrichten am 29.10.2019 (10:07 Uhr) wurde durch eine Filialmitarbeiterin der Beschwerdeführerin im Auftrag ihrer Filialleiterin durchgeführt. Irrtümlich wurde dabei die in Punkt 1.4. angesprochene Datei mit Kundendaten mitübermittelt, die zuvor der Mitarbeiterin von ihrer Filialleiterin zur Verfügung gestellt worden war. 227 Empfänger haben die Nachricht samt Anhang tatsächlich erhalten, bei vier Empfängern kam eine Fehlermeldung (nicht zustellbar) zurück, in drei Fällen konnte die E-Mailzustellung durch das Verwenden der E-Mailrückruffunktion, die sofort nach dem Versand ausgelöst wurde, rückgängig gemacht werden.

In weiterer Folge haben die Mitarbeiterinnen der betroffenen Filiale der Beschwerdeführerin sowohl den unternehmensinternen IT-Support kontaktiert, um mit dessen Hilfe einen Rückruf der zugestellten E-Mails zu veranlassen, was aus technischen Gründen jedoch nicht mehr möglich war. Seitens des ebenfalls kontaktierten (nicht formell bestellten) „Datenschutzbeauftragten der Beschwerdeführerin“ – eigentlich Datenschutzkoordinator der Beschwerdeführerin - erging sodann die Anweisung, den 227 Empfängern eine weitere E-Mail mit dem Inhalt: „Bitte öffnen Sie nicht die von mir verschickte E-Mail, da der Inhalt nicht für Sie bestimmt war. Bitte entschuldigen Sie die Unannehmlichkeiten und bestätigen Sie die Löschung der Nachricht“ zuzusenden. Diese Nachricht wurde 25 Minuten nach dem Versand der ersten Nachricht an dieselben Empfänger verschickt. Durch eine für diesen Vorfall eingerichtete Taskforce konnte spätestens nach 14 Tagen eine Bestätigung über die Löschung

der versendeten E-Mailnachrichten von allen 227 Empfängern per E-Mail bzw. per Telefon eingeholt werden.

1.6. Es besteht eine unternehmensinterne Aufgabenverteilung und interne Arbeitsanweisung dahingehend, wonach die Mitarbeiter einer Filiale die Daten aus der Excel-Datei filtern und sortieren, nicht jedoch zu einer Massensendung verwenden dürfen. Eine solche Massensendung darf demnach nur durch eine spezialisierte und zentrale Stelle der Beschwerdeführerin durchgeführt werden.

Ein explizites Verbot der Durchführung von Massenaussendungen unter Verwendung des E-Mailkontos einzelner Filialmitarbeiterinnen und der BCC-Funktion der E-Mailapplikation (Microsoft Outlook) war der Filialleiterin sowie zumindest einem weiteren Mitarbeiter zum Zeitpunkt des Vorfalls nicht bekannt und hinterfragte die unmittelbar für die Versendung der Datei verantwortliche Mitarbeiterin, welche grundsätzlich Kenntnis einer solchen Arbeitsanweisung hatte, die Dienstanweisung ihrer Vorgesetzten nicht. Die betroffenen Mitarbeiterinnen haben zumindest alle zwei Jahre interne Schulungen zum Datenschutz mit einem positiv Ergebnis abzuschließen.

1.7. Die verfahrensgegenständliche Excel-Datei wurde im oben beschriebenen Umfang bis zu dem Vorfall am 29.10.2019 innerhalb der Netzwerkinfrastruktur auf dem gesicherten Filiallaufwerk in einem passwortgeschützten Ordner verfügbar gehalten. Die Excel-Datei selbst war nicht auf Dateiebene verschlüsselt oder in anderer Form abgesichert. Sie war nicht vollständig anonymisiert oder pseudonymisiert – eine Verbindung der Daten mit konkreten Personen war ohne großen Aufwand auch für einen außenstehenden Dritten möglich. Die Datei wurde etwa monatlich aktualisiert und durch den Geschäftsbereich Marktfolge für zwingend erforderliche interne Arbeitsabläufe bereitgestellt. Aus einer zentralen Datenbank extrahierte ein Mitarbeiter die erforderlichen Kundendaten und erstellt so die Excel-Datei für eine bestimmte Bankfiliale. Der Bereich Marktfolge ist aus aufsichtsrechtlichen Gründen organisatorisch vom Geschäftsbereich Markt (Vertriebseinheiten) zu trennen. Auf die zentrale Datenbank haben dabei nur bestimmte Personen durch ein Berechtigungssystem Zugriff.

1.8. Als unmittelbare Reaktion auf den Sicherheitsvorfall vom 29.10.2019 wurde diese Excel-Datei den Vertriebseinheiten nicht mehr zur Verfügung gestellt und von den Filiallaufwerken gelöscht. Ein vollständiger Verzicht auf die Datei bzw die Liste war jedoch im Geschäftsbetrieb nicht möglich, sodass eine aktualisierte und nun vollständig pseudonymisierte Excel-Liste seit Jänner 2020 wieder auf den Filiallaufwerken zur Verfügung steht. Die Kundenbezeichnung wurde nun durch eine Kunden-ID (ohne ersichtlichen Personenkontext) ersetzt und sämtliche

(Email-)Adressen entfernt. Ein Personenbezug ist nur unter Nutzung einer speziellen internen Eingabemaske zu erzielen und damit für Dritte im Falle eines neuerlichen Verlustes der Daten nicht oder nur mit massivem Aufwand herstellbar. Zudem ist der Zugriff auf die Filialleitung eingeschränkt. Eine Verwendung durch einen Filialmitarbeiter erfordert die Zustimmung der Filialleitung.

1.9. Die technische Ausgestaltung der Datei sowie deren inhaltlicher Umfang wurde weder durch die Vorstände, noch von internen oder externen Datenschutzbeauftragten bzw. sonstigen Experten als Sicherheitsrisiko identifiziert.

1.10. Es war der Beschwerdeführerin bereits zum Zeitpunkt des Sicherheitsvorfalls möglich, die Excel-Liste in der Form zu implementieren, die seit Jänner 2020 Anwendung findet.

1.11. Die Beschwerdeführerin hat unmittelbar nach dem „Data-Breach“ versucht, den Schaden zu minimieren und hat ebenfalls unmittelbar danach die zuständigen Behörden kontaktiert und stets vollständig mit ihnen kooperiert. Die irrtümlich versendete Datei oder Teile davon sind bisher nicht im Internet oder Darknet aufgetaucht.

2. Beweiswürdigung:

2.1. Die Feststellung 1.1. ergibt sich aus den glaubhaften Angaben der Beschwerdeführerin im Laufe des Verfahrens, der in der mündlichen Verhandlung einvernommenen Vorstandsmitglieder am 21.07.2023 und 22.09.2023 sowie dem Jahresbericht 2019 der Beschwerdeführerin.

2.2. Die Feststellung 1.2. ergibt sich aus dem glaubhaften Vorbringen der Beschwerdeführerin im Laufe des erstinstanzlichen Verfahrens, den Aussagen der einvernommenen Vorstandsmitglieder am 21.07.2023 und 22.09.2023, dem Jahresbericht 2019 der Beschwerdeführerin sowie der amtswegigen Recherche des erkennenden Senats zur Unternehmensstruktur der Muttergesellschaft der Beschwerdeführerin. Die DSB hat sämtliche Ermittlungen ausschließlich auf Ebene der Beschwerdeführerin geführt und den Mutterkonzern nicht in das Verfahren einbezogen.

2.3. Die Feststellungen 1.3. und 1.4. ergeben sich aus den übereinstimmenden Vorbringen der Beschwerdeführerin und der Behörde im Laufe des Verfahrens sowie den Zeugenaussagen im erstinstanzlichen Strafverfahren.

2.4. Die Feststellung 1.5. ergibt sich aus übereinstimmenden Vorbringen der Verfahrensparteien im Laufe des Beschwerdeverfahrens.

2.5. Die Feststellung 1.6. ergibt aus der dem Bundesverwaltungsgericht am 15.10.2020 übermittelten Arbeitsanweisung und der dazu veröffentlichten Meldung im internen Unternehmensnetzwerk der Beschwerdeführerin sowie den Aussagen der beiden Vorstandsmitglieder vom 21.07.2023 und 22.09.2023 und des Abteilungsleiters für Finanzen vom 04.07.2023 vor dem Bundesverwaltungsgericht. Die weitere Feststellung betreffend Kenntnisse einzelner Mitarbeiter ergibt sich aus dem vorgelegten Verwaltungsakt, insbesondere den darin enthaltenen Aussagen zweier Filialmitarbeiter sowie der Aussage der Filialleiterin.

2.6. Die Feststellungen 1.7. und 1.8. ergeben sich aus den Ausführungen der Beschwerdeführerin im Laufe des Verfahrens sowie den Aussagen der vernommenen Vorstandsmitglieder und des Leiters der Abteilung für Finanzen vom 21.07.2023, 22.09.2023 und 04.07.2023 in der mündlichen Verhandlung vor dem Bundesverwaltungsgericht.

2.7. Die Feststellungen 1.9. und 1.10. ergeben sich aus den Ausführungen der Beschwerdeführerin im Laufe des Verfahrens sowie den Aussagen der vernommenen Vorstandsmitglieder und dem Abteilungsleiter für Finanzen vom 21.07.2023, 22.09.2023 und 04.07.2023 in der mündlichen Verhandlung vor dem Bundesverwaltungsgericht.

2.8. Die Feststellung 1.11. beruht auf dem vorgelegten Verfahrensakt, den übereinstimmenden Ausführungen der Behörde und der Beschwerdeführerin zum Art. 33 DSGVO Verfahren sowie den Angaben der belangten Behörde im Rahmen eines datenschutzrechtlichen Beschwerdeverfahrens einer betroffenen Bankkundin.

3. Rechtliche Beurteilung:

3.1. Gemäß Art. 130 Abs. 1 Z 1 B-VG entscheiden die Verwaltungsgerichte über Beschwerden gegen den Bescheid einer Verwaltungsbehörde wegen Rechtswidrigkeit.

Gemäß § 6 BVwGG entscheidet das Bundesverwaltungsgericht durch Einzelrichter, sofern nicht in Bundes- oder Landesgesetzen die Entscheidung durch Senate vorgesehen ist.

Gemäß § 27 Abs. 1 DSG entscheidet das Bundesverwaltungsgericht durch Senat über Beschwerden gegen Bescheide, wegen Verletzung der Unterrichtungspflicht gemäß § 24 Abs. 7 leg.cit. und der Entscheidungspflicht der Datenschutzbehörde. Gemäß § 27 Abs. 2 erster Satz DSG besteht der Senat aus einem Vorsitzenden und je einem fachkundigen Laienrichter aus dem Kreis der Arbeitgeber und aus dem Kreis der Arbeitnehmer. Gegenständlich liegt somit Senatszuständigkeit vor.

Das Verfahren der Verwaltungsgerichte mit Ausnahme des Bundesfinanzgerichtes ist durch das VwGVG, BGBl. I Nr. 33/2013, geregelt (§ 1 leg.cit.). Gemäß § 59 Abs. 2 VwGVG bleiben entgegenstehende Bestimmungen, die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bereits kundgemacht wurden, in Kraft.

Gemäß § 17 VwGVG sind, soweit in diesem Bundesgesetz nicht anderes bestimmt ist, auf das Verfahren über Beschwerden gemäß Art. 130 Abs. 1 B-VG die Bestimmungen des AVG mit Ausnahme der §§ 1 bis 5 sowie des IV. Teiles, die Bestimmungen der Bundesabgabenordnung – BAO, BGBl. Nr. 194/1961, des Agrarverfahrensgesetzes – AgrVG, BGBl. Nr. 173/1950, und des Dienstrechtsverfahrensgesetzes 1984 – DVG, BGBl. Nr. 29/1984, und im Übrigen jene verfahrensrechtlichen Bestimmungen in Bundes- oder Landesgesetzen sinngemäß anzuwenden, die die Behörde in dem dem Verfahren vor dem Verwaltungsgericht vorangegangenen Verfahren angewendet hat oder anzuwenden gehabt hätte.

Zu A) I.

3.1.1. Die maßgeblichen Bestimmungen der DSGVO lauten auszugsweise:

Artikel 4 Z 5 und 7:

5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

Artikel 5 - Grundsätze für die Verarbeitung personenbezogener Daten:

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);
(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art. 32 DSGVO - Sicherheit der Verarbeitung:

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:
a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.
(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Artikel 83 - Allgemeine Bedingungen für die Verhängung von Geldbußen:

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.
(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:
a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;

i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und
k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.
(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.
(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:
a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;
b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;
c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.
(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:
a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;
b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
(…)

3.1.2. Die maßgeblichen Bestimmungen des Verwaltungsstrafgesetzes lauten auszugsweise:

§ 5. - Schuld:

(1) Wenn eine Verwaltungsvorschrift über das Verschulden nicht anderes bestimmt, genügt zur Strafbarkeit fahrlässiges Verhalten. Fahrlässigkeit ist bei Zuwiderhandeln gegen ein Verbot oder bei Nichtbefolgung eines Gebotes dann ohne weiteres anzunehmen, wenn zum Tatbestand einer Verwaltungsübertretung der Eintritt eines Schadens oder einer Gefahr nicht gehört und der Täter nicht glaubhaft macht, daß ihn an der Verletzung der Verwaltungsvorschrift kein Verschulden trifft.
(1a) Abs. 1 zweiter Satz gilt nicht, wenn die Verwaltungsübertretung mit einer Geldstrafe von über 50 000 Euro bedroht ist.

(2) Unkenntnis der Verwaltungsvorschrift, der der Täter zuwidergehandelt hat, entschuldigt nur dann, wenn sie erwiesenermaßen unverschuldet ist und der Täter das Unerlaubte seines Verhaltens ohne Kenntnis der Verwaltungsvorschrift nicht einsehen konnte.

§ 10. Strafen:

(1) Strafart und Strafsatz richten sich nach den Verwaltungsvorschriften, soweit in diesem Bundesgesetz nicht anderes bestimmt ist.
(2) Soweit für Verwaltungsübertretungen, insbesondere auch für die Übertretung ortspolizeilicher Vorschriften, keine besondere Strafe festgesetzt ist, werden sie mit Geldstrafe bis zu 218 Euro oder mit Freiheitsstrafe bis zu zwei Wochen bestraft.

§ 19. - Strafbemessung:

(1) Grundlage für die Bemessung der Strafe sind die Bedeutung des strafrechtlich geschützten Rechtsgutes und die Intensität seiner Beeinträchtigung durch die Tat.
(2) Im ordentlichen Verfahren (§§ 40 bis 46) sind überdies die nach dem Zweck der Strafdrohung in Betracht kommenden Erschwerungs- und Milderungsgründe, soweit sie nicht schon die Strafdrohung bestimmen, gegeneinander abzuwägen. Auf das Ausmaß des Verschuldens ist besonders Bedacht zu nehmen. Unter Berücksichtigung der Eigenart des Verwaltungsstrafrechtes sind die §§ 32 bis 35 des Strafgesetzbuches sinngemäß anzuwenden. Die Einkommens- und Vermögensverhältnisse und allfällige Sorgepflichten des Beschuldigten sind bei der Bemessung von Geldstrafen zu berücksichtigen.

§ 33a. - Beratung

(1) Stellt die Behörde eine Übertretung fest und sind die Bedeutung des strafrechtlich geschützten Rechtsgutes und die Intensität seiner Beeinträchtigung durch die Tat und das Verschulden des Beschuldigten gering, so hat ihn die Behörde, soweit die Verwaltungsvorschriften nicht anderes bestimmen, mit dem Ziel einer möglichst wirksamen Beendigung des strafbaren Verhaltens oder der strafbaren Tätigkeiten zu beraten und ihn schriftlich unter Angabe der festgestellten Sachverhalte aufzufordern, innerhalb einer angemessenen Frist den den Verwaltungsvorschriften und behördlichen Verfügungen entsprechenden Zustand herzustellen.
(2) Wird der schriftlichen Aufforderung innerhalb der von der Behörde festgelegten oder erstreckten Frist entsprochen, dann ist die weitere Verfolgung einer Person wegen jener Übertretungen, betreffend welche der den Rechtsvorschriften und behördlichen Verfügungen entsprechende Zustand hergestellt worden ist, unzulässig.
(3) Die Intensität der Beeinträchtigung des strafrechtlich geschützten Rechtsgutes ist jedenfalls nicht gering, wenn die Übertretung nachteilige Auswirkungen auf Personen oder Sachgüter bewirkt hat oder das Auftreten solcher Auswirkungen bei auch nur kurzem Andauern des strafbaren Verhaltens oder der strafbaren Tätigkeiten zu erwarten ist.

(4) Die Intensität der Beeinträchtigung des strafrechtlich geschützten Rechtsgutes gilt als gering, wenn geringfügige Abweichungen von technischen Maßen festgestellt wurden und keine der im Abs. 3 genannten Umstände vorliegen.
(5) Abs. 1 und 2 sind jedenfalls nicht anzuwenden auf
1. Übertretungen von Verwaltungsvorschriften, die zur Strafbarkeit vorsätzliches Verhalten erfordern;
2. Übertretungen, die innerhalb der letzten drei Jahre vor Feststellung der Übertretung bereits Gegenstand einer Beratung und schriftlichen Aufforderung durch die Behörde waren oder zu denen einschlägige noch nicht getilgte Verwaltungsstrafen bei der Behörde aufscheinen;
3. Übertretungen, die Anlass zu in den Verwaltungsvorschriften vorgesehenen einstweiligen Zwangs- und Sicherungsmaßnahmen geben;
4. Übertretungen, für welche die Verwaltungsvorschriften die Maßnahme der Entziehung von Berechtigungen vorsehen.

§ 64 – Kosten des Strafverfahrens:

(1) In jedem Straferkenntnis ist auszusprechen, daß der Bestrafte einen Beitrag zu den Kosten des Strafverfahrens zu leisten hat.
(2) Dieser Beitrag ist für das Verfahren erster Instanz mit 10% der verhängten Strafe, mindestens jedoch mit 10 Euro zu bemessen; bei Freiheitsstrafen ist zur Berechnung der Kosten ein Tag Freiheitsstrafe gleich 100 Euro anzurechnen. Der Kostenbeitrag fließt der Gebietskörperschaft zu, die den Aufwand der Behörde zu tragen hat.
(3) Sind im Zuge des Verwaltungsstrafverfahrens Barauslagen erwachsen (§ 76 AVG), so ist dem Bestraften der Ersatz dieser Auslagen aufzuerlegen, sofern sie nicht durch Verschulden einer anderen Person verursacht sind; der hienach zu ersetzende Betrag ist, wenn tunlich, im Erkenntnis (der Strafverfügung), sonst durch besonderen Bescheid ziffernmäßig festzusetzen. Dies gilt nicht für Gebühren, die dem Dolmetscher und Übersetzer zustehen, der dem Beschuldigten beigestellt wurde.
(4) Von der Eintreibung der Kostenbeiträge (Abs. 1 und § 54d) und der Barauslagen ist abzusehen, wenn mit Grund angenommen werden darf, daß sie erfolglos wäre.
(5) Die §§ 14 und 54b Abs. 1, 1a und 1b sind sinngemäß anzuwenden.
(6) Wird einem Antrag des Bestraften auf Wiederaufnahme des Strafverfahrens nicht stattgegeben, so gelten hinsichtlich der Verpflichtung zur Tragung der Verfahrenskosten sinngemäß die vorhergehenden Bestimmungen.

3.2. Anwendung der Rechtsgrundlage auf den konkreten Fall:

3.2.1. Strafbarkeit einer juristischen Person und Verfolgungsverjährung:

Der EuGH führte zur Strafbarkeit der juristischen Person in der Rechtssache C-807/21 folgendes aus:

„Insbesondere geht aus dem zehnten Erwägungsgrund der DSGVO hervor, dass deren Bestimmungen u. a. die Ziele haben, bei der Verarbeitung personenbezogener Daten unionsweit ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und zu diesem Zweck sicherzustellen, dass die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten dieser Personen bei der Verarbeitung solcher Daten unionsweit gleichmäßig und einheitlich angewendet werden. Es liefe diesem Zweck der DSGVO jedoch zuwider, den Mitgliedstaaten zu gestatten, einseitig und als erforderliche Voraussetzung für die Verhängung einer Geldbuße gemäß Art. 83 DSGVO gegen einen Verantwortlichen, der eine juristische Person ist, zu verlangen, dass der betreffende Verstoß zuvor einer identifizierten natürlichen Person zugerechnet wurde oder ihr zuzurechnen ist. Außerdem könnte eine solche zusätzliche Anforderung letztlich unter Verstoß gegen Art. 83 Abs. 1 DSGVO die Wirksamkeit und die abschreckende Wirkung von Geldbußen schwächen, die gegen juristische Personen als Verantwortliche verhängt werden. Es ist mit Blick auf die Fragen des vorlegenden Gerichts festzustellen, dass der Begriff „Unternehmen" im Sinne der Art. 101 und 102 AEUV ohne Bedeutung für die Frage ist, ob und unter welchen Voraussetzungen eine Geldbuße nach Art. 83 der DSGVO gegen einen Verantwortlichen verhängt werden kann, der eine juristische Person ist, da diese Frage in Art. 58 Abs. 2 und Art. 83 Abs. 1 bis 6 DSGVO abschließend geregelt ist. Nach alledem ist auf die erste Frage zu antworten, dass Art. 58 Abs. 2 Buchst. i und Art. 83 Abs. 1 bis 6 DSGVO dahin auszulegen sind, dass sie einer nationalen Regelung entgegenstehen, wonach eine Geldbuße wegen eines in Art. 83 Abs. 4 bis 6 DSGVO genannten Verstoßes gegen eine juristische Person in ihrer Eigenschaft als Verantwortliche nur dann verhängt werden kann, wenn dieser Verstoß zuvor einer identifizierten natürlichen Person zugerechnet wurde. Insoweit ist zu der Frage, ob ein Verstoß vorsätzlich oder fahrlässig begangen wurde und aufgrund dessen mit einer Geldbuße gemäß Art. 83 DSGVO geahndet werden kann, noch klarzustellen, dass ein Verantwortlicher für ein Verhalten, das in den Anwendungsbereich der DSGVO fällt, sanktioniert werden kann, wenn er sich über die Rechtswidrigkeit seines Verhaltens nicht im Unklaren sein konnte, gleichviel, ob ihm dabei bewusst war, dass es gegen die Vorschriften der DSGVO verstößt. Handelt es sich bei dem Verantwortlichen um eine juristische Person, ist zudem klarzustellen, dass die Anwendung von Art. 83 DSGVO keine Handlung und nicht einmal eine Kenntnis seitens des Leitungsorgans dieser juristischen Person voraussetzt. Nach alledem ist auf die zweite Frage zu antworten, dass Art. 83 DSGVO dahin auszulegen ist, dass nach dieser Bestimmung eine Geldbuße nur dann verhängt werden darf, wenn nachgewiesen ist, dass der Verantwortliche, der eine juristische Person und zugleich ein Unternehmen ist, einen in Art. 83 Abs. 4 bis 6 DSGVO genannten Verstoß vorsätzlich oder fahrlässig begangen hat." (EuGH 05.12.2023, (Deutsche Wohnen SE) C-807/21)

Daraus folgt, dass entgegen dem Vorbringen der Beschwerdeführerin – das sich auf die damalige (mittlerweile allerdings modifizierte) Judikatur des Verwaltungsgerichtshofes bezieht – eine juristische Person Beschuldigte in einem Verwaltungsstrafverfahren sein kann, ohne dass die Datenschutzverletzung zuvor einer natürlichen Person aus dem Kreis des Unternehmens zuzurechnen ist (§ 9 VStG, § 30 DSG). Die ständige Rechtsprechung des Verwaltungsgerichtshofes zur Strafbarkeit von juristischen Personen im Verwaltungsstrafverfahren kann daher nicht länger aufrechterhalten werden und ist alleine bzw. mit dem abschließenden Katalog des Art. 83 DSGVO eine Strafbarkeit herzustellen, wobei zwingend ein Verschulden in der Form des Vorsatzes oder der Fahrlässigkeit gefordert wird. Dies bedeutet jedoch nicht, dass eine Handlung oder eine Kenntnis seitens des Leitungsorgans der juristischen Person vorausgesetzt wird. Die diesen Ausführungen widersprechenden nationalen Reglungen in § 9 VStG und § 30 DSG haben bei der Beurteilung des gegenständlichen Falls unangewendet zu bleiben (Erga omnes – Wirkung von Urteilen des Europäischen Gerichtshofes). Die Behandlung des weiteren Vorbringens der Beschwerdeführerin zu diesem Themenkomplex konnte somit unterbleiben. Aus diesem Grund geht auch das Vorbringen der Beschwerdeführerin hinsichtlich einer bereits eingetreten Verfolgungsverjährung ins Leere.

3.2.2. Zur Eigenschaft der Beschwerdeführerin als Verantwortliche:

Beim Verantwortlichen handelt es sich um jene Person oder Einrichtung, die dafür zu sorgen hat, dass die Datenschutzbestimmungen der DSGVO eingehalten werden. Damit gilt der Verantwortliche als Adressat der Pflichten aus der DSGVO und der Begriff dient der Zuweisung von Verantwortlichkeiten. Der Verantwortliche ist Adressat von Ansprüchen der betroffenen Person und gilt als Ansprechstelle für Maßnahmen der Aufsichtsbehörde (ErwGr 74). (*Hödl in Knyrim, DatKomm Art 4 DSGVO Rz 77 (Stand 1.12.2018, rdb.at)*)

Die Rolle des für die Verarbeitung Verantwortlichen definiert sich durch drei Merkmale:
1. jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle (personenbezogener Aspekt),
2. die allein oder gemeinsam mit anderen (pluralistische Kontrolle),
3. über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden (Entscheidungsfunktion). (*Hödl in Knyrim, DatKomm Art 4 DSGVO Rz 80 (Stand 1.12.2018, rdb.at)*)

Die Verantwortung wird dem übertragen, der die Entscheidungsmacht hat. Entscheidend für die Zuweisung der Verantwortlichkeit ist daher, wer über die wesentlichen Aspekte der Mittel

der Verarbeitung entscheidet. Für die Zuschreibung der Verantwortlichen-Eigenschaft ist es nicht erforderlich, dass der Verantwortliche selbst Daten verarbeitet, sich im Besitz der verarbeiteten Daten befindet oder über die physische Herrschaft verfügt. Trifft er die Entscheidung, dass Daten zu verarbeiten sind, sind ihm sämtliche Personen und Stellen funktional zuzurechnen, die unter seiner Aufsicht bzw Anweisung Schritte einer Datenverarbeitung vornehmen (Hilfsorgane). Sofern natürliche Personen Daten für ihre eigenen Zwecke außerhalb des Tätigkeitsbereichs und der möglichen Kontrolle ihrer Organisation verarbeiten, können sie selbst Verantwortlicher werden. Es kann aber zur Mitverantwortung einer fährlässig handelnden Organisation kommen, die einen Datenmissbrauch grundsätzlich zu verhindern hat. *(Hödl in Knyrim, DatKomm Art 4 Rz 83, 86, DSGVO (Stand 1.12.2018, rdb.at*))

Weiters enthält Art 83 das „Modell der unmittelbaren Verbandshaftung“, ein Haftungsmodell für juristische Personen „sui generis“, wonach das dahinterstehende Unternehmen für das Zuwiderhandeln seiner Mitarbeiter haftbar ist. Dies deshalb, um auch nicht-identifizierbares oder nicht direkt rückführbares Verhalten der juristischen Person zuordnen und deren Haftung anordnen zu können. Kompetenzüberschreitungen einzelner handelnder Personen sollten allerdings nicht zuzurechnen sein, wenn der Handelnde die Funktion und Grenzen eindeutig überschreitet und dem Unternehmen auch nicht anderweitig zugerechnet werden kann. (*Illibauer in Knyrim, DatKomm Art 83 Rz 20 DSGVO (Stand 1.12.2021, rdb.at)*)

Soweit die Beschwerdeführerin kurzzeitig behauptete, nicht Verantwortliche der gegenständlichen Datenverarbeitung zu sein, sondern die betreffenden Mitarbeiter, welche den Verarbeitungsvorgang physisch ausgelöst hätten, kann dem nichts abgewonnen werden. So ist eindeutig, dass Unternehmen im Rahmen von Art. 83 DSGVO für Datenschutzverstöße eines jeden Beschäftigten haften, wenn der Mitarbeiter nicht im Exzess (für eigene Zwecke) gehandelt hat. Ein solcher Fall der Haftung eines einzelnen Arbeitnehmers wäre bspw dann gegeben, wenn Datensätze des Arbeitgebers genutzt würden, um private Zwecke zu verfolgen. Dies ist bereits bei oberflächlicher Betrachtung der verfahrensgegenständlichen Datenverarbeitung auszuschließen. So führte sowohl die in die Datenschutzverletzung involvierte Filialleiterin, als auch die die Verarbeitung auslösende Filialmitarbeiterin die Datenverarbeitung im Rahmen ihres Arbeitsverhältnisses im Interesse der Beschwerdeführerin durch. Ein falsch versendeter Anhang vermag dran nichts zu ändern, auch wenn dies durch eine irrtümliche – jedenfalls fahrlässige – individuelle Handlung einer Mitarbeiterin erfolgte.

Dazu kommt, dass für die grundsätzliche Konfiguration und (fehlende) Absicherung des relevanten Datensatzes unstrittig nicht die in der Filiale tätigen Mitarbeiterinnen, sondern die Leitungsorgane der Beschwerdeführerin zuständig sind.

Da die Eigenschaft als Verantwortliche für die Filialleiterin und die betroffene Filialmitarbeiterin bereits aus diesem Grund ausscheidet und die Beschwerdeführerin während des Großteils des Beschwerdeverfahrens ihre Eigenschaft als Verantwortliche im Sinne des Art. 4 Z 7 DSGVO bejaht, ist nicht im Detail auf die weiteren Voraussetzungen einzugehen. Fest steht, dass es sich bei der Beschwerdeführerin um eine juristische Person handelt, welche im gegenständlichen Fall alleine und mit Entscheidungsgewalt – über die wesentlichen Aspekte der Zwecke und Mittel der Verarbeitung – u.a. durch Weisungen, entscheidet. Die Beschwerdeführerin ist somit Verantwortliche gemäß Art. 4 Z 7 DSGVO.

3.2.3. Zur Strafbarkeit und Strafbemessung (Art. 83 Abs. 4 lit a DSGVO iVm § 32 DSGVO und Art. 5 Abs. 1 lit f DSGVO):

Schon vor Geltung der DSGO wurde die Datensicherheit zu den Grundsätzen des Datenschutzrechts gezählt. Mit Art 5 Abs 1 lit f wurde dies nunmehr ausdrücklich normiert. Wie bereits aus dem Wortlaut deutlich wird, geht dies über die Vertraulichkeit hinaus und umfasst den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Unbefugte können nicht nur sonstige Dritte, sondern auch Mitarbeiter des Verantwortlichen sein. Abgestellt wird jedoch nicht nur auf – äußere oder interne – „Angreifer“, sondern auch auf unbeabsichtigte Ereignisse. Der Begriff Integrität kann mit Unverfälschtheit oder Unversehrtheit umschrieben werden und bedeutet, dass die Daten nicht von Unbefugten oder sonst unbeabsichtigt verändert oder gelöscht werden dürfen. Mit anderen Worten ist Integrität dann gegeben, wenn die Daten in dem Zustand sind, den der letzte zu ihrer Modifikation Berechtigte hergestellt hat. Vertraulichkeit bedeutet, dass Daten nicht von Unbefugten gelesen oder verarbeitet werden dürfen. Diese sog Schutzziele sind durch geeignete technische und organisatorische Maßnahmen umzusetzen. In Art 32 wird dies entsprechend konkretisiert. Dort sind neben der Integrität und der Vertraulichkeit auch die Schutzziele der Verfügbarkeit und der Belastbarkeit erwähnt. Art 5 Abs. 1 lit f fordert einen angemessenen Schutz. Damit ist eine Abwägung angesprochen, die insb die Risiken für die Betroffenen betrachtet und durch die in Art 32 normierten Kriterien näher ausgestaltet ist. Der Einsatz angemessener Datensicherheitsmaßnahmen ist dabei eine Verpflichtung des Verantwortlichen sowie des Auftragsverarbeiters, subjektive Rechtsansprüche einer betroffenen Person ergeben sich allein daraus nach der Rsp aber keine, wenn nicht bereits ein

bestimmtes Betroffenenrecht nach Art 15–22 verletzt wurde. (*Hötzendorfer/Tschohl/Kastelitz in Knyrim, DatKomm Art 5 Rz 54-56 DSGVO (Stand 7.5.2020, rdb.at)*)

Art. 32 Abs 1 fordert in Bezug auf die Sicherheit der Verarbeitung, dass unter Berücksichtigung des Stands der Technik („State of the Art“) sowie der Implementierungskosten je nach der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie der Wahrscheinlichkeit und der Höhe des Risikos für die persönlichen Rechte und Freiheiten geeignete technische und organisatorische Maßnahmen (TOM) vom Verantwortlichen und vom Auftragsverarbeiter zu treffen sind, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Art 83 enthält die allgemeinen Bedingungen für die Verhängung von Geldbußen, die von der nationalen Aufsichtsbehörde verhängt werden. Gem Art 83 Abs 4 lit a können bei Verstößen gegen die Bestimmungen des Art 32 der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter mit einer Geldbuße von bis zu 10 Mio Euro oder im Fall eines Unternehmens von bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden, je nachdem, welcher der Beträge höher ist. (*Pollirer in Knyrim, DatKomm Art 32 Rz 3, 10 DSGVO (Stand 1.5.2022, rdb.at)*)

Als erstes Kriterium für die Zielerreichung, nämlich die Erreichung eines dem Risiko angemessenen Schutzniveaus, fordert Art. 32 Abs 1 die Berücksichtigung des Stands der Technik, als zweites Kriterium die Berücksichtigung der Implementierungskosten für die Umsetzung der technischen und organisatorischen Maßnahmen, als drittes Kriterium für die Zielerreichung die Art, den Umfang, die Umstände und den Zweck der Datenverarbeitung und als viertes Kriterium ist die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen vom für die Verarbeitung Verantwortlichen zu beachten.

Wie oben bereits festgestellt wurde am 29.10.2019 aus einer Filiale der Beschwerdeführerin eine E-Mailnachricht an 227 Empfänger (tatsächlich) zugestellt, der irrtümlich eine unverschlüsselte interne Excel-Liste mit nicht vollständig anonymisierten Kundendaten (jedenfalls offensichtlich erkennbare Nachnamen und abgekürzte Vornamen natürlicher Personen sowie den korrespondierenden E-Mailadressen, welche in einem Kontext mit dem Einkommen und Vermögen dieser identifizierten bzw. mit einfachen Mitteln identifizierbaren Personen stehen) beigeschlossen war, wobei ein Personenbezug im Sinne des Art. 4 Z 1 DSGVO unzweifelhaft vorliegt. Dies erfolgte unter Verletzung interner Arbeitsanweisungen zur Emailkultur, welche zum Zeitpunkt der Datenschutzverletzung bereits im internen

Nachrichtenportal der Beschwerdeführerin veröffentlicht waren. Unmittelbar verantwortlich für die Verbreitung der Liste waren die Filialleiterin und eine Filialmitarbeiterin, welche die Versendung der verfahrensgegenständlichen E-Mailnachrichten einleiteten bzw. durchführten. Der Fehler wurde unmittelbar darauf erkannt und mit einer sofortigen Schadensabwendung bzw. Schadensminimierung begonnen (siehe Feststellungen). Die Beschwerdeführerin hat in diesem Zusammenhang gegenüber der Behörde stets kooperiert und die Details ihrer Arbeitsprozesse und Motive freiwillig offengelegt. Die auf dem Filiallaufwerk liegende Excel-Datei wurde in Reaktion auf diesen Vorfall vom Filialserver gelöscht, bei der Beschwerdeführerin zunächst gesperrt und erst nach vollständiger Pseudonymisierung wieder intern zur Verfügung gestellt. Es gibt bis zum heutigen Tag keinen Hinweis, dass die hier gegenständliche Excel-Datei im Internet kursieren würde oder von Dritten genutzt worden wäre.

Auf Basis dieser Ausführungen im Rahmen des Verwaltungsstrafverfahrens und der Entscheidung des EuGH vom 05.12.2023 (C-807/21) ist eine juristische Person (wie die Beschwerdeführerin) direkt als Beschuldigte im Verfahren heranzuziehen und führte die belangte Behörde dieses gegen die korrekte Beschuldigte.

Der belangten Behörde ist weiteres zuzustimmen, wenn sie ausführt, dass die soeben dargestellte und festgestellte Vorgehensweise zum Zeitpunkt der Datenschutzverletzung gegen Art. 5 Abs. 1 lit f DSGVO und Art. 32 DSGVO verstößt und in Folge den Straftatbestand des Art. 83 Abs. 4 lit a DSGVO erfüllt. Die rechtliche Beurteilung ist, mit Ausnahme der Begründung des Verschuldens, zutreffend und ändert die Rechtsprechung des EuGH zu C-807/21 grundsätzlich nichts an dieser Einschätzung.

Nicht zu folgen ist in diesem Zusammenhang dem Vorbringen der Beschwerdeführerin, die Konfiguration der Liste wäre sicherheitstechnisch „state of the art“ gewesen und/oder die Implementierung einer besseren Absicherung nicht zumutbar. Dabei wird seitens des Gerichts nicht in Zweifel gezogen, dass die hier in Rede stehende Dateikonfiguration auch bei anderen vergleichbaren Instituten üblich war. Das ändert aber nichts an dem Umstand, dass eine enorme Steigerung der Datensicherheit durch einen vergleichsweise geringen Mehraufwand (Streichung der e-mail, vollständige Pseudonymisierung der Kundenkennung) erreicht werden konnte und auch schon vor dem hier relevanten Vorfall problemlos erfolgen hätte können. Das ergibt sich schon aus dem Umstand, dass eben dieser Schritt unmittelbar nach dem Vorfall binnen kurzer Zeit umgesetzt werden konnte. Der entstandene Mehraufwand bei der Datenbearbeitung ist dabei überschaubar.

Vor diesem Hintergrund ist als „state of the art“ jedenfalls nicht eine ungesicherte Datei mit einfach zu identifizierenden personenbezogenen Daten anzusehen (die nur durch interne Anweisungen „gesichert“ ist), sondern eben die nunmehr in Verwendung stehende vollständig pseudonymisierte Kundendatei, die unabhängig von einer zusätzlichen Verschlüsselung bei Verlust keine Verbindung zu konkreten Personen durch Dritte ermöglicht. Eine solche Datei dann noch gesondert zusätzlich zu schützen, ist jedoch nicht erforderlich.

Eine verschuldensunabhängige Haftung kommt nicht in Frage und ist stets Vorsatz oder Fahrlässigkeit eine zwingende Voraussetzung zur Erfüllung des Straftatbestands des Art. 83 Abs. 4 lit a DSGVO. Soweit die Beschwerdeführerin ein Verschulden bestreitet und dies insbesondere mit der fehlenden Informationen an die mittlere Führungsebene bzw. den Vorstand und mit den ohne Ergebnis gebliebenen internen und externen Datenschutzüberprüfungen argumentiert, ist darauf hinzuweisen, dass nach der neuen Rechtsprechung die Anwendung von Art. 83 DSGVO keine Handlung und nicht einmal eine Kenntnis seitens des Leitungsorgans einer juristischen Person voraussetzt. Vielmehr ist objektiv zu beurteilen, ob der juristischen Person ein Verschulden an der erfolgten Datenschutzverletzung vorzuwerfen ist.

Angesichts der vorgebrachten und durchgeführten (belegten) internen Schulungen sowie Ablaufsregelungen (welche einen wichtigen Bestandteil der Sorgfaltspflichten der Beschwerdeführerin bilden), gegen die die Filialmitarbeiterinnen verstoßen haben, ist die von der DSB angenommene „mangelnde Kontrolle und Überwachung“ nicht nachvollziehbar. Daran ändert auch der Umstand nichts, dass den Filialmitarbeiterinnen offenbar nicht alle Regelungen, etwa zu „Massen-E-mails“, bekannt waren. Es wäre eine Massenversendung von Ostergrüßen nämlich ebenfalls nach den internen Regelungen unzulässig – datenschutzrechtlich aber völlig irrelevant. Das datenschutzrechtliche Problem entstand in diesem Fall erst durch die im Anhang mitübermittelte Kundendatei. Daran, dass deren Versendung den Mitarbeiterinnen als unzulässig bekannt war, besteht jedoch nicht der geringste Zweifel, weil unmittelbar darauf bereits das Problem gemeldet und die Schadensminimierung eingeleitet wurde.

Darüber hinaus liegt aber auch ein Verschulden – im Sinne einer leichten Fahrlässigkeit – in dem Umstand, dass seitens der Beschwerdeführerin eine nicht vollständig pseudonymisierte Excel-Datei für Arbeitsprozesse zur Verfügung gestellt wurde, die offensichtlich technisch problemlos (auf Filialebene) in einem Massenemail exportiert werden konnte. Dass ein solcher Export grundsätzlich untersagt war, kann der Feststellung einer leichten Fahrlässigkeit nicht entgegenstehen, weil eine unbeabsichtigte Offenlegung einer solchen Datei, die

regelmäßig in Arbeitsprozessen Eingang gefunden hat, zumindest als potenzielles Risiko nicht ausgeschlossen werden kann.

Der belangten Behörde ist daher im Ergebnis nicht zu widersprechen, wenn sie die Strafbarkeit der Beschwerdeführerin bejaht.

3.2.4. Zur Strafbemessung und dem Unternehmensbegriff:

Der EuGH (C-807/21) führte zur Bemessung der zu verhängenden Strafe gegen eine juristische Person, wegen eines unter Art. 83 DSGVO subsumierbaren Verstoßes in den Randziffern 56 bis 59 folgendes aus:

„56 Dieser Unternehmensbegriff umfasst für die Zwecke der Anwendung der in den Art. 101 und 102 AEUV niedergelegten Wettbewerbsregeln jede eine wirtschaftliche Tätigkeit ausübende Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung. Er bezeichnet somit eine wirtschaftliche Einheit, auch wenn diese aus rechtlicher Sicht aus mehreren natürlichen oder juristischen Personen besteht. Diese wirtschaftliche Einheit besteht in einer einheitlichen Organisation persönlicher, materieller und immaterieller Mittel, die dauerhaft einen bestimmten wirtschaftlichen Zweck verfolgt (Urteil vom 6. Oktober 2021, Sumal, C-882/19, EU:C:2021:800, Rn. 41 und die dort angeführte Rechtsprechung).

57 So ergibt sich aus Art. 83 Abs. 4 bis 6 DSGVO, der die Berechnung der Geldbußen für die in diesen Absätzen aufgeführten Verstöße betrifft, dass, wenn der Adressat der Geldbuße ein Unternehmen im Sinne der Art. 101 und 102 AEUV ist oder einem solchen angehört, der Höchstbetrag für die Geldbuße auf der Grundlage eines Prozentsatzes des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs des betreffenden Unternehmens berechnet wird.

58 Letztlich kann, wie der Generalanwalt in Nr. 47 seiner Schlussanträge ausgeführt hat, nur eine Geldbuße, deren Höhe anhand der tatsächlichen oder materiellen Leistungsfähigkeit des Adressaten von der Aufsichtsbehörde unter Zugrundelegung des Begriffs der wirtschaftlichen Einheit im Sinne der in Rn. 56 des vorliegenden Urteils angeführten Rechtsprechung festgesetzt wird, die drei in Art. 83 Abs. 1 DSGVO genannten Voraussetzungen erfüllen, sowohl wirksam und verhältnismäßig als auch abschreckend zu sein.

59 Daher ist eine Aufsichtsbehörde, wenn sie aufgrund ihrer Befugnisse nach Art. 58 Abs. 2 DSGVO beschließt, gegen einen Verantwortlichen, der ein Unternehmen im Sinne der Art. 101 und 102 AEUV ist oder einem solchen angehört, eine Geldbuße gemäß Art. 83 DSGVO zu verhängen, nach Art. 83 im Licht des 150. Erwägungsgrundes der DSGVO verpflichtet, bei der

Berechnung der Geldbußen für die in Art. 83 Abs. 4 bis 6 DSGVO genannten Verstöße den Begriff „Unternehmen" im Sinne der Art. 101 und 102 AEUV zugrunde zu legen."

Konkret stellt sich die Frage, ob zwischen der Beschwerdeführerin, welche eine (beinahe) einhundertprozentige Tochter der Muttergesellschaft ist, von einer wirtschaftlichen Einheit im Sinne der oben erwähnten Judikatur zu Art. 101 und 102 AEUV auszugehen ist. Dies kann aufgrund der nachstehenden Erwägung nicht angenommen werden:

Der dem europäischen Wettbewerbsrecht zugrundeliegende Begriff des Unternehmens ist jede eine wirtschaftliche Tätigkeit ausübende Einheit (*erstmal EuGH 23.04.1991, (Höfner) C-41/90 Rz 21*), wobei eine wirtschaftliche Tätigkeit im Anbieten von Gütern oder Dienstleistungen auf einem Markt besteht (*vgl. EuGH 12.09.2000, (Pavlov) C-180/98*). Im vorliegenden Fall ist es unstrittig, dass die Beschwerdeführerin als konzessioniertes Kreditinstitut Dienstleistungen auf einem Markt anbietet und war daher nur auf den Begriff der „eine wirtschaftliche Tätigkeit ausübende Einheit" näher einzugehen.

Aus der oben genannten Rechtsprechung ergibt sich, dass als entscheidendes Kriterium das Vorhandensein eines einheitlichen Verhaltens auf einem Markt heranzuziehen ist, ohne dass die formale Trennung zwischen verschiedenen Unternehmen, die sich aus der Verschiedenheit ihrer Rechtspersönlichkeiten ergibt, eine solche Einheit für die Anwendung der Wettbewerbsregeln ausschließen kann (*vgl. EuGH 14.07.1972, (Imperial Chemical Industries/Kommission) C-48/69*). Der Begriff „Unternehmen" umfasst somit jede eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung, und bezeichnet somit eine wirtschaftliche Einheit, auch wenn diese aus rechtlicher Sicht aus mehreren natürlichen oder juristischen Personen besteht (*vgl. EuGH 10.09.2009, (Akzo Nobel u. a./Kommission) C-97/08 P Rz 54 und 55*). Diese wirtschaftliche Einheit besteht in einer einheitlichen Organisation persönlicher, materieller und immaterieller Mittel, die dauerhaft einen bestimmten wirtschaftlichen Zweck verfolgt (*vgl. EuGH 01.07.2010, (Knauf Gips/Kommission) C-407/08 P, Rz 84 und 86*).

Verstößt eine solche wirtschaftliche Einheit gegen Wettbewerbsnormen oder (wie hier relevant) die Bestimmungen der DSGVO, so hat sie nach dem Grundsatz der persönlichen Haftung für diese Zuwiderhandlung einzustehen. So kann nach der Rechtsprechung einer Muttergesellschaft das Verhalten ihrer Tochtergesellschaft insbesondere dann zugerechnet werden, wenn die Tochtergesellschaft trotz eigener Rechtspersönlichkeit ihr Marktverhalten zum Zeitpunkt der Begehung der Zuwiderhandlung nicht selbständig bestimmt, sondern im Wesentlichen Weisungen der Muttergesellschaft befolgt, und zwar vor allem wegen der

wirtschaftlichen, organisatorischen und rechtlichen Beziehungen, die die beiden Rechtssubjekte verbinden, so dass sie in einem solchen Fall zur selben wirtschaftlichen Einheit gehören und damit ein einziges Unternehmen bilden, das Urheber der Zuwiderhandlung ist (*vgl. in diesem Sinne EuGH 10.09.2009, (Akzo Nobel u. a./Kommission), C-97/08 P, Rn. 58 und 59*).

Die Abhängigkeit des Marktverhaltens ist die Grundvoraussetzung für die wirtschaftliche Einheit. Dabei gilt auch bei einer Beteiligung von (nahezu) 100 Prozent die (widerlegbare) Vermutung für eine solche fehlende Unabhängigkeit, ohne dass weitere Indizien beizubringen sind. Wenn jedoch die Tochtergesellschaft eigenständig am Markt auftritt und selbstbestimmt handelt, ist (ohne das die Höhe der Beteiligung eine Rolle spielt) eine wirtschaftliche Einheit abzulehnen. Durch dieses funktionale Verständnis des Unternehmensbegriffs gelingt es, das Vorliegen nur eines einzigen Unternehmens zum Zeitpunkt eines Rechtsverstoßes zu begründen, dass sich aus der Mutter- und den abhängigen Tochtergesellschaften zusammensetzt und welches für die Rechtsverletzung einzustehen hat. (*Forgo/Helfrisch/Schneider, Betrieblicher Datenschutz[3] Rechtshandbuch, 1488 Rz 91-92*)

Richtig ist zwar, dass im Kontext des Art 83 DSGVO ein Unternehmensbegriff, wie er im EU-Kartellrecht geprägt wurde („wirtschaftliche Einheit“; vgl bspw EuGH 18.07.2013, Rs C-501/11 P, Rn 101-104), zugrunde gelegt werden soll (vgl idS ErwGr 150 Satz 3 DSGVO). (…) Eine Übertragung dieses Konzepts auf Datenschutzverstöße würde bedeuten, dass danach zu fragen wäre, ob und in welchem Ausmaß eine Konzernmutter Einfluss auf Datenverarbeitungsstrategien der Töchter nimmt. Beschränkte sich eine Mutter bspw auf die reine Beteiligungsverwaltung iS eines Finanzinvestors, ohne auf operative Entscheidungen der Töchter Einfluss zu nehmen, erschiene es unplausibel für DSGVO-Verstöße einer Tochter den gesamten Konzern verantwortlich zu machen. Anders zu beurteilen wäre dagegen der Fall, dass die Konzernmutter bspw eine Tochter mit der konzernweiten Erbringung bestimmter Dienstleistungen beauftragt (Bsp: Verwaltung der Daten von Führungskräften zwecks Personalplanung). *(Kunnert, Datenschutz in Fragen & Antworten, 124 Frage 22)*

Sinn und Zweck der Sanktionsregelungen ist, dass große Unternehmen von Verstößen gegen die Verordnung general- und spezialpräventiv abgehalten werden. Dies kann nur gelingen, wenn für multinationale Weltkonzerne die Sanktionen auch spürbar sind. Könnten sie die Datenverarbeitung in umsatzschwache Tochterfirmen ausgliedern und so die Geldbuße verringern, wäre dieses Ziel nicht erreicht. *(Simitis/Hornung/Spiecker, Datenschutzrecht, 1220 Rz 43)*

Es ist daher das Verhältnis der Beschwerdeführerin zu ihrer Muttergesellschaft in wirtschaftlicher, organisatorischer und rechtlicher Hinsicht zu beurteilen. In dieser Hinsicht kann nicht verkannt werden, dass es sich bei der Beschwerdeführerin um eine (beinahe) einhundertprozentige Tochter der Muttergesellschaft handelt und damit die widerlegbare Vermutung aufgestellt wird, dass es sich um eine wirtschaftliche Einheit handelt. Dabei wird auch nicht übersehen, dass in rechtlicher Hinsicht eine Abhängigkeit von der Muttergesellschaft dahingehend besteht, dass grundlegende Entscheidungsfindungen auf Konzernebene stattfinden, jedoch die Beschwerdeführerin mit einer eigenen Führungsebene, welche bis zu einem Vorstand reicht, ausgestattet ist. So bleibt auch unbestritten, dass strategische Konzerninteressen nicht durch die Beschwerdeführerin entschieden werden, während die wie im vorliegenden Fall relevanten Geschäftszweige dieser selbst überlassen sind. Im gegenständlichen Fall ist dabei zu berücksichtigen, dass es sich bei der Muttergesellschaft um eine Holdinggesellschaft handelt, in der die Beschwerdeführerin ein Teil eines in sie eingebrachten Verbundes vergleichbarer Institute mit gemeinsamen Produkten aber grundsätzlich in eigener Verantwortung (und mit eigener Bilanz) agiert.

Es besteht zudem ein gesondertes Filialnetz zwischen der Beschwerdeführerin und der Muttergesellschaft, welches auch in personeller Hinsicht durch die Beschwerdeführerin selbst geführt wird. Die Beschwerdeführerin ist Teil eines Haftungsverbundes mit einer größeren Zahl an gleich oder ähnlich strukturierten Instituten mit lokalem Schwerpunkt, welcher in den letzten 30 Jahren systematisch in die Muttergesellschaft integriert worden ist. Daraus ergeben sich gewisse personelle Verflechtungen, jedoch bewahren die Institute ein eigenständiges Auftreten auf dem Markt. Auch besteht zwar im Konzern ein gemeinsamer Datenschutzbeauftragter; es sind allerdings auch verantwortliche Beauftragte auf Unternehmens- beziehungsweise Filialebene installiert, insbesondere auch für den Bereich „Datenschutz“.

Ausgehend von der oben zitierten Darstellung bei Kunnert liegt die Konstellation bei der Beschwerdeführerin zwischen den dargestellten klaren Polen. Insbesondere unterscheidet sie sich aber auch grundlegend von der Konstellation bei „Deutsche Wohnen“, wo die Konzernmutter das gesamte operative Geschäft an Tochtergesellschaften ausgelagert hat (siehe C-807/21, RN 11).

Zwischen der Beschwerdeführerin und der Muttergesellschaft besteht somit keine „wirtschaftliche Einheit“ im hier relevanten Verständnis. Auslöser des gegenständlichen Verfahrens war ein individueller Fehler auf Filialebene in Verbindung mit einer datenschutzrechtlich problematischen Datei, die ein eigenständiges Produkt der

Beschwerdeführerin war – somit die reine Unternehmensebene betrifft – und in keinem Zusammenhang mit der Muttergesellschaft steht (zum Unternehmensbegriff siehe auch *Jahnel/Pallwein-Prettner, Datenschutzrecht 219f*). Dies hat sich auch klar im erstinstanzlichen Verfahren gezeigt, in dem die Datenschutzbehörde ausschließlich die Filial- und Unternehmensebene einbezogen hat, nicht aber (auch nicht im datenschutzrechtlichen Kontext) den Mutterkonzern.

Es war daher das Betriebsergebnis der Beschwerdeführerin von gerundet EUR 146,6 Millionen dem heranziehenden Strafrahmen zu Grunde zu legen.

Wie oben bereits ausgeführt, ist es unionsrechtlich geboten, bei einem Verstoß gegen Art. 83 Abs. 4 bis 6 DSGVO, der die Geldbußen für die in diesen Absätzen aufgeführten Verstöße betrifft, den Höchstbetrag für die Geldbuße auf der Grundlage eines Prozentsatzes des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (gerundet 146,6 Millionen Euro) der betroffenen juristischen Person zu ermitteln. Wobei insbesondere bei der Beurteilung der Höhe der zu verhängenden Strafe, auf die tatsächliche oder materielle Leistungsfähigkeit des Adressaten abzustellen ist, jedoch diese sowohl wirksam, verhältnismäßig als auch abschreckend sein muss.

Im vorliegenden Fall stellt Art. 32 DSGVO im Verhältnis zu Art. 5 Abs. 1 lit. f DSGVO (Grundsätze der Datenverarbeitung) die speziellere Norm dar und war die verhängte Geldbuße anhand des Strafrahmens des – letztlich auch für die Verantwortliche günstigeren – Art. 83 Abs. 4 lit. a DSGVO festzusetzen. Der Strafrahmen reicht somit gemäß Art. 83 Abs. 4 DSGVO bis zu einem Betrag von EUR 10.000.000.

Das Bundesverwaltungsgericht hat ergänzend die Leitlinien 04/2022 des Europäischen Datenschutzausschusses als Berechnungsgrundlage herangezogen, die bei – hier gegebenem geringem Schweregrad („low level of seriousness“) – und der oben festgehaltenen Umsatzgröße einen statischen Strafrahmen von bis zu EUR 500.000 annehmen, wobei der konkrete Umsatz im unteren Drittel der Bandbreite (100 Millionen bis 250 Millionen Euro) liegt.

Art. 83 Abs. 2 DSGVO sieht im Rahmen der Strafbemessung die folgenden (im gegenständlichen Fall heranzuziehenden) Kriterien vor:

a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

c) jegliche von dem Verantwortlichen getroffene Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
d) Grad der Verantwortung des Verantwortlichen unter Berücksichtigung der von ihm gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
e) etwaige einschlägige frühere Verstöße des Verantwortlichen;
f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche den Verstoß mitgeteilt hat;
k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

Die Strafbemessung innerhalb eines gesetzlichen Strafrahmens ist eine Ermessensentscheidung, die nach den vom Gesetzgeber im § 19 VStG festgelegten Kriterien vorzunehmen ist (VwGH 05.09.2013, 2013/09/0106).

Grundlage für die Bemessung der Strafe sind die Bedeutung des strafrechtlich geschützten Rechtsguts und die Intensität seiner Beeinträchtigung durch die Tat (§ 19 Abs. 1 VStG). Überdies sind die in Betracht kommenden Erschwerungs- und Milderungsgründe gegeneinander abzuwägen. Auf das Ausmaß des Verschuldens ist besonders Bedacht zu nehmen. Unter Berücksichtigung der Eigenart des Verwaltungsstrafrechts sind die §§ 32 bis 35 des Strafgesetzbuches sinngemäß anzuwenden. Die Einkommens- und Vermögensverhältnisse und allfällige Sorgepflichten des Beschuldigten sind bei der Bemessung von Geldstrafen zu berücksichtigen (§ 19 Abs. 2 VStG).

Gemäß Art. 83 Abs. 2 lit a DSGVO ist wohl einerseits die Höhe des eingetretenen Schadens als auch die Zahl der vom Verstoß betroffenen Personen und die Auswirkungen bzw das Risiko für ihre Rechte und Freiheiten zu werten. Auch die zeitliche Komponente spielt eine Rolle. Nach der Artikel-29-Datenschutzgruppe spielt auch eine Rolle, ob überhaupt ein Schaden entstanden ist. (*Illibauer in Knyrim, DatKomm Art 83 DSGVO Rz 68-69 (Stand 1.12.2021, rdb.at)*)

Als erschwerend konnte aufgrund des zugrundeliegenden Sachverhalts lediglich die Art des Verstoßes unter Berücksichtigung der Anzahl der Betroffenen und der systematischen Verarbeitung bankspezifischer Daten durch die Beschwerdeführerin als Kreditinstitut gewertet werden, da Daten wie das Einkommen einem größeren Personenkreis offengelegt wurden. Eine besondere Schwere ist nicht erkennbar, da insbesondere kein nennenswerter

Schaden entstanden ist, die personenbezogenen Daten nicht im Internet oder Darknet aufgetaucht und keine sonstigen konkreten Auswirkungen feststellbar sind.

Auch ergibt sich – anders als im Straferkenntnis der DSB ausgeführt – keine besondere Schwere aus der Aufrechterhaltung bzw. Weiterführung der gleichen „riskanten“ Praxis durch die Wiedereinführung der überarbeiteten Excel-Liste in Kombination mit einem strikten Zugriffsmanagement. So ist es insbesondere ausgeschlossen, dass über die seit Jänner 2020 und auch aktuell genutzte – vollständig pseudonymisierte – Excel-Datei weiterhin die Herstellung eines Personenbezugs durch Dritte (im Falle eines Datenverlustes) ermöglicht wäre.

Damit im Zusammenhang steht auch das in Summe vorbildliche Krisenmanagement und das rasche Agieren der Beschwerdeführerin im Rahmen der erfolgten Datenschutzverletzung und konnte die Dauer des effektiven „Data Breach“ auf einen kurzen Zeitraum von ungefähr 14 Tagen beschränkt werden, da von allen Empfängern der verfahrensgegenständlichen Excel-Liste binnen 14 Tagen eine Bestätigung über die Vernichtung bzw. Löschung des E-Mails eingeholt werden konnte. Dies geschah im Rahmen einer eigens eingerichteten „Taskforce“ der Beschwerdeführerin, um jegliche negative Folgen für betroffene Personen abzuwenden.

Der Beschwerdeführerin kann als Verantwortliche der verfahrensgegenständlichen Datenverarbeitungen nur eine „leichte Fahrlässigkeit“ hinsichtlich der Verwendung einer nicht pseudonymisierten Liste zugerechnet werden, da keine Vorfälle, Indikatoren sowie interne oder externe Prüfer auf eine entsprechende Gefahr hingewiesen haben und auch sonst den grundsätzlichen Schulungspflichten im Umgang mit personenbezogenen Daten nachgekommen wurde. Eine auffallende Sorglosigkeit ist nicht erkennbar, vielmehr handelt es sich um ein Fehlverhalten der Beschwerdeführerin im Sinne einer (noch) leichten Fahrlässigkeit, weil bei einer sorgsamen Evaluierung erkannt hätte werden müssen, dass trotz der technischen Möglichkeit zur Pseudonymisierung der in Rede stehenden Excel-Liste/Datei, dies unterlassen wurde. Ob die Beschwerdeführerin dabei (auffallend) sorgloser agiert hätte als vergleichbare Institute, wurde im Straferkenntnis nicht thematisiert. Auch auf die „Vorgeschichte“ der Entstehung der Datei wird nicht eingegangen.

Vor diesem Hintergrund kann auch den Ausführungen der DSB, wonach es „keine bis völlig unzureichende Schutzmaßnahmen“ für die Finanzdaten und daher eine „enorme Gefahr“ für die Rechte der betroffenen Personen gegeben hätte, nicht gefolgt werden. Diesen liegt zu Grunde, dass die DSB das unglückliche Zusammenwirken von Nachlässigkeiten (leichter Fahrlässigkeit) zweier Filialmitarbeiterinnen – einerseits schon das interne Verschicken der

Datei ohne entsprechenden Hinweis durch die Filialleiterin, anderseits das irrtümliche Weiterverschicken dieser Datei als Anhang an 234 Kunden – gewissermaßen als Standardrisiko annimmt, weshalb konsequenterweise die fehlende Sicherung der Datei durch Passwort oder Pseudonymisierung besonders problematisiert wird. Dabei wird dann erschwerend zurückgerechnet, wie lange die Datei in dieser Form (ohne unbeabsichtigt offengelegt zu werden) bereits in Verwendung stand. Diese Dateien wurden immer erst auf Anfrage generiert und am Filialserver zur Verfügung gestellt – sie lagen nicht dauerhaft zum freien Zugriff aller Mitarbeiter bereit.

In der Logik der Behörde (Straferkenntnis, Seite 29 / 4.7.) wäre es der Beschwerdeführerin (massiv) zu Gute gekommen, wäre der „Data Breach“ bereits kurz nach Einführung der (nicht-pseudonymisierten) Datei erfolgt. Dies kann bei einer Strafbemessung in Fällen eines fahrlässigen „Anlagefehlers“ bei der grundsätzlichen Konfiguration eines Datensatzes – anders als bei einem Vorsatzdelikt – nur eingeschränkt herangezogen werden. Aus Sicht des Gerichts ist es nämlich nicht dem (glücklichen) Zufall zu verdanken, dass die Datei erst nach längerer Zeit im Einsatz unabsichtlich offengelegt wurde, sondern vielmehr dem Umstand, dass das Schulungssystem in Bezug auf Datenschutz grundsätzlich funktioniert hat und in Verbindung mit den internen Anweisungen ein angemessenes Schutzniveau hergestellt hat. Wie schon ausgeführt, war es den involvierten Filiallmitarbeiterinnen auch stets bewusst, dass sie die Datei keinesfalls an Dritte hätten verschicken dürfen.

Insofern ist die Missachtung oder Unkenntnis der Regeln für den Massenversand von E-Mails im gegenständlichen Fall auch nicht von jener Bedeutung, die ihr die DSB zumisst. Denn der Kern des Straferkenntnisses – die fehlende Pseudonymisierung der Datei – wäre auch bei einer Offenlegung an mehrere Personen unterhalb der Schwelle des Massenversandes zum Tragen gekommen. Und in diesem Fall wären die entsprechenden Regelungen gar kein Thema gewesen.

Schließlich hat sich im gerichtlichen Beschwerdeverfahren – wie ebenfalls bereits ausgeführt – ergeben, dass die Datensätze seit Jänner 2020 vollständig pseudonymisiert und damit jedenfalls hinreichend gesichert sind.

Zusätzlich ist – wie bereits seitens der DSB im Straferkenntnis – mildernd zu berücksichtigen, dass keinerlei einschlägige frühere Verstöße gegen die DSGVO aufscheinen, die Beschwerdeführerin im Rahmen des Ermittlungsverfahrens vor der Datenschutzbehörde und dem Bundesverwaltungsgericht kooperativ mitgewirkte, die Datenschutzverletzung durch die Beschwerdeführerin im Rahmen von Art. 33 DSGVO selbst gemeldet wurde, ein

Zugriffsberechtigungssystem sowie technische Maßnahmen für die Verhinderung von Datenschutzverletzungen implementiert waren (wenn auch nicht auf Dateiebene) und die Beschwerdeführerin einen wesentlichen Beitrag zur Wahrheitsfindung leistete.

Auf dieser Basis war im Rahmen einer Abwägung die Höhe der Geldstrafe deutlich im unteren Bereich des Strafrahmens anzusetzen. Unbestritten ist dabei, dass aus generalpräventiven, aber auch spezialpräventiven Gründen im Sinne einer Sensibilisierung die Verhängung einer Strafe erforderlich ist. Das Beschwerdeverfahren lieferte keine Anhaltspunkte von der Berechnungsmethode des EDPB abzugehen. Dabei wird der Schweregrad „leicht“, welcher sich aus der soeben ausgeführten Strafbemessung ergibt und das Betriebsergebnis der Beschwerdeführerin als eigenständige wirtschaftliche Einheit in der Höhe von (gerundet) EUR 146,6 Millionen herangezogen.

Für den gegenständlichen Fall eines Verstoßes gemäß Art. 83 Abs. 4 DSGVO mit einem lediglich leichten Schweregrad erweist sich eine Strafe in der Höhe von EUR 50.000 als schuld- und tatangemessen, zumal die Beschwerdeführerin in der Verhandlung auch bereits eine erhöhte Sensibilisierung im Zusammenhang mit den datenschutzrechtlichen Anforderungen glaubhaft machen konnte. Im Übrigen hat auch die DSB ihre Strafe („am untersten Ende des zur Verfügung stehenden Strafrahmens“) angesetzt.

Schließlich erweist sich die verhängte Strafe auch aus wirtschaftlicher Sicht verhältnismäßig, aber auch als hinreichend abschreckend für die Beschwerdeführerin, da ihr bewusst sein muss, dass wesentliche Milderungsgründe bei einem erneuten Verstoß nicht mehr schlagend werden. Dies gilt im Sinne der Generalprävention entsprechend auch für vergleichbare Institute.

3.2.5. Zur Aussetzung des Beschwerdeverfahrens:

Hat eine Behörde (ein VwG) dem EuGH eine Frage zur Vorabentscheidung nach Art 267 AEUV vorgelegt, so dürfen gemäß § 38a Abs. 1 AVG (iVm § 17 VwGVG) bis zum Einlangen der Vorabentscheidung nur solche Handlungen vorgenommen oder Entscheidungen und Verfügungen getroffen werden, die durch die Vorabentscheidung nicht beeinflusst werden können oder die die Frage nicht abschließend regeln und keinen Aufschub gestatten (vgl auch den praktisch gleichlautenden § 38b Abs. 1 zweiter Satz VwGG). Damit sollte eine Regelung getroffen werden, „wie vorzugehen ist, wenn beim Gerichtshof der Europäischen Gemeinschaften eine Vorabentscheidung beantragt wird“ (RV 1995, 8). Demgemäß nimmt die hL an, dass innerstaatlich lediglich § 38a AVG ein Organ iSd Art 267 AEUV, das selbst ein Vorabentscheidungsersuchen an den EuGH gestellt hat, ermächtigt und dieses gleichzeitig

verpflichtet, mit der Entscheidung in dieser Sache bis zur Erledigung des Vorabentscheidungsersuchens zuzuwarten. (*Hengstschläger/Leeb, AVG § 38a Rz 12 (Stand 1.4.2021, rdb.at))*

Demgegenüber hat der VwGH zwar auch in diesem Zusammenhang das Vorliegen einer Vorfrage iSd § 38 AVG ausdrücklich davon abhängig gemacht, dass „der Tatbestand ein Element enthält“, welches für sich allein Gegenstand der bindenden Entscheidung einer anderen Behörde ist (VwGH 31. 1. 2003, 2002/02/0158), dennoch aber insofern einen weiten Vorfragenbegriff entwickelt. Nach seiner stRsp bildet nämlich die Frage, wie Unionsrecht auszulegen ist (vgl VwGH 20. 2. 2003, 2001/16/0518; 26. 6. 2003, 98/18/0334; 26. 4. 2011, 2011/03/0015), einschließlich der Frage, ob es unmittelbar anwendbar ist (VwGH 29. 1. 2003, 99/03/0151) und innerstaatliches Recht verdrängt (VwGH 4. 3. 1999, 98/16/0166; 31. 1. 2003, 2002/02/0158; 3. 7. 2003, 2000/15/0137), eine (solche) Vorfrage, weil sie zufolge des Auslegungsmonopols des EuGH in Angelegenheiten des primären und sekundären Unionsrechts von einem (diesem) Gericht zu entscheiden ist. (*Hengstschläger/Leeb, AVG § 38 Rz 17 (Stand 1.4.2021, rdb.at)*)

Mit dieser Rsp gibt der VwGH zu erkennen, dass er den Vorabentscheidungsurteilen des EuGH Bindungswirkung nicht nur für den vorgelegten, sondern auch für alle gleich gelagerten Fälle beimisst (VfSlg 18.797/2009). Sie hat die – praktisch begrüßenswerte – Auswirkung (siehe zB VwGH 26. 4. 2011, 2011/03/0015), dass auch letztinstanzliche Gerichte iSd Art 267 Abs. 3 AEUV nicht genötigt sind, dem EuGH die gleiche Frage noch einmal vorzulegen. Ferner ist es bei dieser Auslegung nicht notwendig, § 38a AVG (auf den der VwGH in seinen Entscheidungen nicht Bezug nimmt; vgl auch § 38b VwGG), der seinem Wortlaut nach nur für das Ausgangsverfahren gilt (vgl auch Sharaf, ÖZW 2008, 65), in im Hinblick auf das Effizienzprinzip (vgl insb § 39 Abs 2 letzter Satz AVG) teleologischer Interpretation bzw. analog auch auf solche Verfahren anzuwenden. Dies scheint im Ergebnis deshalb zweckmäßig, weil damit gewährleistet ist, dass die Säumnis nur durch einen nach außen tretenden Akt (entweder Vorabentscheidungsersuchen oder förmliche Aussetzung gemäß § 38 AVG abgewendet werden kann. (*Hengstschläger/Leeb, AVG § 38 Rz 19 (Stand 1.4.2021, rdb.at)*)

Praktisch bedeutsamer ist § 38a AVG damit im aktuellen Rechtsschutzsystem für die VwG, für die er zum einen gem § 17 VwGVG (bzw § 38 VwGVG iVm § 24 VStG) sinngemäß gilt und die zum anderen auch Gerichtsqualität iSd Art 267 AEUV aufweisen (VwGVG § 29 Rz 14; VfSlg 19.896/2014; Eberhard/Ranacher/Weinhandl, ZfV 2020, 299; vgl auch VwGH 8. 10. 2020, Ra 2020/06/0177). (*Hengstschläger/Leeb, AVG § 38a Rz 3 (Stand 1.4.2021, rdb.at)*)

In seiner ursprünglichen Fassung BGBl 1995/471 nahm § 38a AVG seinem Wortlaut nach darauf Bezug, dass „eine auf Grund der einschlägigen gemeinschaftsrechtlichen Vorschriften hiefür in Betracht kommende Behörde“ beim EuGH „einen Antrag auf Fällung einer Vorabentscheidung gestellt“ hat. Auch auf die Entscheidungserheblichkeit der Vorlage kam es daher nach dem Wortlaut des § 38a Abs. 1 AVG aF, der lediglich an das (objektive) Faktum der Antragstellung anknüpfte, wohl nicht an (idS auch VwSlg 15.560 A/2001 [Rz 13]). In diesem Sinn dürfte auch der Umformulierung durch die Nov BGBl I 2011/100 – wonach es darauf ankommt, dass die Behörde eine Frage „nach Art. 267 [AEUV] vorgelegt“ hat – keine Bedeutung zukommen, zumal ihrer Entstehungsgeschichte kein Anhaltspunkt zu entnehmen ist, dass damit eine Änderung der Rechtslage beabsichtigt war. (*Hengstschläger/Leeb, AVG § 38a Rz 12 (Stand 1.4.2021, rdb.at)*)

Nach dem ersten Tatbestand des § 38a Abs 1 AVG können daher solche verfahrensleitenden Anordnungen und Bescheide bzw förmliche Entscheidungen der VwG ergehen, die überhaupt nicht von der Lösung der Frage, die dem EuGH zur Vorabentscheidung vorgelegt wurde, betroffen sind. Dazu können nicht nur Akte innerhalb des Verwaltungsverfahrens bzw verwaltungsgerichtlichen Verfahrens, wie z.B. die Anordnung der Aufnahme bestimmter Beweise, … gezählt werden. (*Hengstschläger/Leeb, AVG § 38a Rz 15 (Stand 1.4.2021, rdb.at)*)

§38a AVG trifft keine ausdrückliche Regelung für den Fall, dass auf Grund der Vorlage durch ein anderes Gericht bereits ein Vorabentscheidungsverfahren beim EuGH über dieselbe Auslegungsfrage anhängig ist. Das Effizienzprinzip sowie das unionsrechtliche Auslegungsmonopol des Europäischen Gerichtshof verpflichtet die Behörde oder das Gericht jedoch dazu, die Entscheidung des EuGH abzuwarten. Nach der Rechtsprechung des VwGH kann in diesem Fall gemäß § 38 AVG mit Aussetzung des Verfahrens vorgegangen werden (VwGH 09.11.2011, 2011/22/0284).

Wie den oben dargestellten rechtlichen Ausführungen zur Entstehungsgeschichte des § 38a AVG zu entnehmen ist, kann nicht davon ausgegangen werden kann, dass der Gesetzgeber mit der veränderten Wortfolge im Vergleich zur Stammfassung eine Einschränkung auf „die tatsächlich vorlegende Behörde oder das vorlegende Gericht gemäß Art. 267 AEUV“ etablieren wollte. Dies ergibt sich bereits aus dem Grundsatz der Verfahrensökonomie und der identen Ausgangslage der Verfahren.

Es sind auch keine Anhaltspunkte ersichtlich, welche eine sinngemäße Anwendung des § 38a AVG auf eine Aussetzung, betreffend eine anhängige präjudizielle Vorfrage beim Europäischen Gerichtshof, ausschließen würden. So handelt es sich um ständige Rechtsprechung des

Verwaltungsgerichtshofes, dass Urteile des EuGH über den Ausgangsfall hinaus eine bindende Wirkung entfallen und alle Behörden und Gerichten diese bei der Entscheidungsfindung zu berücksichtigen haben. In diesem Zusammenhang war daher mit einer Aussetzung gemäß Art. 38 AVG (wie dies gegenständlich der Fall war) vorzugehen, weil die Frage der Strafbarkeit der juristischen Person (in Abweichung von der bisherigen Rechtsprechung des VwGH) im gegenständlichen Verfahren grundlegend entscheidend war. Wenn umgekehrt davon ausgegangen werden müsste, dass ein aussetzendes Gericht zwingend alle Verfahrenshandlungen zu unterlassen hätte, auch wenn diese nicht im Zusammenhang mit der durch den EuGH zu beurteilenden Vorfrage/unionsrechtlichen Frage stehen und ausschließlich der Sachverhaltserhebung oder davon gänzlich unabhängiger Rechtsfragen dienen, käme es zu einer strukturellen Benachteiligung jener Gerichte, welche aus Gründen der Effizienz, Verfahrensökonomie und Entlastung des Europäischen Gerichtshofes kein eigenes Vorabentscheidungsersuchen stellen, da ein ähnlicher (präjudizieller) Fall ohnehin bereits anhängig ist. Ein solches Ergebnis wäre mit den Grundsätzen des Verwaltungsverfahrens, insbesondere jener des Verwaltungsstrafverfahrens, nicht vereinbar.

In diesem Zusammenhang ist darauf hinzuweisen, dass die im Rahmen des Verwaltungsstrafverfahrens zu beachtenden Fristen (u.a. § 34 Abs. 1 VwGVG, § 43 Abs. 1 VwGVG) während des ausgesetzten Beschwerdeverfahrens bis zur Entscheidung des Europäischen Gerichtshofes in der Rechtssache C-807/21 gehemmt waren und keine faktische Forstsetzung des Beschwerdeverfahrens stattgefunden hat. Das Beschwerdeverfahren war demnach nicht einzustellen und ist das Straferkenntnis der belangten Behörde nicht außer Kraft getreten. Da die Beschwerdeführerin die gegenständliche Beschwerde am 17.03.2021 eingebracht, das Bundesverwaltungsgericht mit Beschluss vom 18.05.2022 das Verfahren in Bezug auf ein Vorabentscheidungsverfahren des EuGH betreffend (ausschließlich) die Frage der Erlassung eines Straferkenntnis in Bezug auf eine juristische Person ausgesetzte und der Europäische Gerichthof das vorgelegte Verfahren am 05.12.2023 mit Urteil entschieden hat, weshalb die Aussetzung damit ex lege beendet wurde, ist die Entscheidungsfrist für das Bundesverwaltungsgericht zum Entscheidungszeitpunkt offen. Die während der Aussetzung durchgeführten Verfahrensschritte des Gerichts standen nicht im Zusammenhang mit dem Gegenstand des Vorabentscheidungsverfahrens.

Schließlich sprechen auch ganz praktische Erwägungen und Interessen der Verfahrensparteien gegen eine restriktive Auslegung der während einer Aussetzung zulässigen Ermittlungsschritte. Einerseits kann das Gericht das Verfahren in solchen Fällen regelmäßig sehr rasch nach der Entscheidung des EuGH abschließen. Andererseits ergibt sich die Möglichkeit, Beweiserhebungen – und insbesondere Zeugenbefragungen – so zu

terminisieren, dass sie ein Eingehen auf Vertagungsbitten oder das Berücksichtigen sonstiger Interessen der Beschwerdeführer, etwa wesentliche Geschäftstermine, ermöglichen. Beides ist im gegenständlichen Verfahren auch substanziell schlagend geworden und konnten etwa wichtige geschäftliche Termine der betroffenen Vorstände problemlos berücksichtigt werden.

3.2.6. Zum sonstigen Beschwerdevorbringen:

Soweit die Beschwerdeführerin in ihrer Beschwerde vorbrachte, das Straferkenntnis verstoße gegen § 44a Z 1 VStG, es sei der Begriff der Integrität unrichtig beurteilt worden, die § 11 DSG und § 33a VStG unangewendet geblieben, es habe die belangte Behörde das Parteiengehör der Beschwerdeführerin verletzt, und es sei das verfassungsgesetzlich verankerte Bestimmtheitsgebot durch Art. 5 Abs. 1 lit f DSGVO nicht erfüllt, kann dem aus folgenden Gründen nichts abgewonnen werden:

So ist festzustellen, dass die Anwendung des § 11 DSG im Ermessen der belangten Behörde liegt und allein deshalb kein Recht auf Anwendung einer Verwarnung besteht. Im Rahmen der durch das Bundesverwaltungsgericht neu durchführten Strafbemessung war keine Veranlassung zum Vorgehen gemäß § 11 DSG zu erblicken. Soweit die Beschwerdeführerin moniert, dass die belangte Behörde nicht nach § 33a VStG vorgegangen ist, übersieht jene, dass § 33a Abs. 3 VStG ein solches Vorgehen ausschließt, wenn die Übertretung nachteilige Auswirkungen auf Personen oder Sachgüter bewirkt hat oder das Auftreten solcher Auswirkungen bei auch nur kurzem Andauern des strafbaren Verhaltens oder der strafbaren Tätigkeiten zu erwarten ist. Letztes ist auf den gegenständlichen Sachverhalt anwendbar.

Der Beschwerdeführerin ist zuzustimmen, dass der Spruch die Anführung des Zeitpunktes der Begehung der Tat und, falls es sich um einen Zeitraum handelt, dessen Anfang und Ende in einer kalendermäßig eindeutig umschriebenen Art zu umfassen hat (VwGH 22. 2. 2006, 2005/17/0195; 20. 11. 2008, 2007/09/0255; s auch VwGH 19. 3. 2014, 2013/09/0030; 24. 3. 2020, Ra 2019/09/0123; ferner VwGH 21. 7. 2022, Ra 2022/04/0018). Jedoch ist die im Straferkenntnis vorgeworfene und auslösende Tathandlung (Versenden der Excel-Liste als Anhang einer E-Mailnachricht betreffend die Einladung zum Weltspartag bei gleichzeitiger Verwendung einer nicht vollständig pseudonymisierten Excel-Datei im Arbeitsablauf durch die Beschwerdeführerin) jedenfalls kalendermäßig ausgesprochen.

Auch kann dem Vorbringen der Beschwerdeführerin zum Begriff der Integrität gemäß Art. 5 Abs. 1 lit f DSGVO nichts abgewonnen werden und erweist sich die Beurteilung der belangten Behörde als korrekt. Die Verarbeitungsgrundsätze des Art. 5 DSGVO werden durch weitere Bestimmungen der DSGVO konkretisiert, dies trifft auf Art. 32 DSGVO zu. So sind die

Schutzziele des Verarbeitungsgrundsatzes durch geeignete technische und organisatorische Maßnahmen umzusetzen und dies in Art 32 entsprechend konkretisiert. (*Hötzendorfer/Tschohl/Kastelitz in Knyrim, DatKomm Art 5 Rz 56 DSGVO (Stand 7.5.2020, rdb.at)*)

Ebenso ergibt sich keine Verletzung des verfassungsgesetzlich verankerten Bestimmtheitsgebots. Tat, Täter und Tatumstände wurden hinreichend präzise beschrieben. Darüber hinaus darf ein Spruch nicht durch ein Übermaß an inhaltlichen beweiswürdigenden Erwägungen überfrachtet werden. Schließlich wurde der gesonderte Tatbestand der weiterführenden Verwendung einer nicht (vollständig) pseudonymisierten Datei in der gegenständlichen Beschwerdeentscheidung ohnehin vollständig verworfen.

Eine allfällige Verletzung des Parteiengehörs im erstinstanzlichen Verfahren wurde jedenfalls durch Einsicht im Rahmen des Beschwerdeverfahrens sowie die umfassende mündliche Beschwerdeverhandlung saniert.

3.2.8. Mündliche Abweisung von Beweisanträgen am 21.12.2023

Die Notwendigkeit der Beziehung eines IT-Sachverständigen konnte in der Verhandlung am 21.12.2023 erneut nicht schlüssig begründet werden. Insbesondere konnte die Beschwerdeführerin angesichts der umgehend nach dem „Data Breach“ erfolgten Pseudonymisierung der Kundendatei nicht darlegen, dass dies aus technischen Gründen vorher nicht möglich gewesen wäre. Gleiches gilt für die beantragte Befragung eines einschlägig fachkundigen Zeugen.

Auch die Befragung der übrigen beantragten Zeugen erweist sich für die Feststellung des entscheidungsrelevanten Sachverhalts als nicht erforderlich, weil dieser aus Sicht des Gerichts bereits hinreichend geklärt werden konnte und sie teilweise auch nur für Themenkomplexe erfolgten, die vom Gericht ohnehin nicht weiter verfolgt oder anders gesehen wurden, als im Erkenntnis der Datenschutzbehörde – etwa die Einbeziehung der Konzernmutter, weil ohnehin auf den Umsatz der Beschwerdeführerin abgestellt wurde.

3.2.7. Zu den Kosten des behördlichen und gerichtlichen Verwaltungsstrafverfahrens:

Nach Neubemessung der Strafhöhe, war der gemäß § 64 Abs. 1 und 2 VStG auszusprechende Beitrag zu den Kosten des Strafverfahrens neu festzusetzen. Dieser beträgt 10% der verhängten Strafe, mindestens jedoch EUR 10 und war daher spruchgemäß mit EUR 5.000 zu bestimmen. Ein Beitrag zu den Kosten des verwaltungsgerichtlichen Verfahrens war nicht

auszusprechen, da gemäß § 52 Abs. 8 VwGVG der Beschwerde hinsichtlich der Strafhöhe Folge gegeben wurde.

Zu B) Zulässigkeit der Revision:

Gemäß § 25a Abs. 1 VwGG hat das Verwaltungsgericht im Spruch seines Erkenntnisses oder Beschlusses auszusprechen, ob die Revision gemäß Art. 133 Abs. 4 B-VG zulässig ist. Der Ausspruch ist kurz zu begründen.

Die Revision ist gemäß Art. 133 Abs. 4 B-VG zulässig, weil die Entscheidung von der Lösung einer Rechtsfrage abhängt, der grundsätzliche Bedeutung zukommt, weil die gegenständliche Entscheidung von der bisherigen Rechtsprechung des Verwaltungsgerichtshofes abweicht bzw. es an einer höchstgerichtlichen Rechtsprechung fehlt. Infolge des Urteils des EuGH vom 05.11.2023 (C-807/21) kann die bisherige Judikatur des Verwaltungsgerichtshofes, hinsichtlich der Strafbarkeit von juristischen Personen, nicht länger aufrechterhalten werden. Darüber hinaus fehlt es an höchstgerichtlicher Judikatur zur Frage der heranzuziehenden Bemessungsgrundlage bei Geldstrafen gemäß Art. 83 DSGVO – insbesondere im Zusammenhang mit einem reinen Unternehmenssachverhalt – und es ist die Revision auch zur Frage der erlaubten Ermittlungsmöglichkeiten eines Gerichts während eines ausgesetzten Verfahrens zulässig.