



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

0 3 . 0 6 . 2 0 2 4

G E S C H Ä F T S Z A H L

W 2 9 2 2 2 8 2 2 8 4 - 1 / 1 0 E

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

Das Bundesverwaltungsgericht hat durch den Richter Mag. Herwig ZACZEK als Vorsitzenden und die fachkundigen Laienrichter Mag.^a Huberta MAITZ-STRAßNIG und Mag. Matthias SCHACHNER als Beisitzer über die Beschwerde von XXXX , vertreten durch Reif und Partner Rechtsanwälte OG, gegen das Straferkenntnis der Datenschutzbehörde vom 02.11.2023, Zl. D550.853 / 2023-0.749.445, nach Durchführung einer öffentlichen mündlichen Verhandlung am 31.01.2024, zu Recht erkannt:

A)

I. Der Beschwerde hinsichtlich des Ausspruches über die verhängte Strafe wird teilweise Folge gegeben und die zu den Spruchpunkten I. bis III. des bekämpften Straferkenntnisses verhängte Geldstrafe auf EUR 4.000,00 (Ersatzfreiheitsstrafe im Fall der Uneinbringlichkeit: 224 Stunden) herabgesetzt. Korrespondierend dazu reduziert sich der Beitrag zu den Kosten des Strafverfahrens vor der belangten Behörde gemäß § 64 VStG auf (gesamt) EUR 400,00 und der zu zahlende Gesamtbetrag, auf EUR 4.400,00.

II. Gemäß § 52 Abs. 8 VwGVG hat die Beschwerdeführerin keine Kosten des verwaltungsgerichtlichen Verfahrens zu tragen.

III. Im Übrigen wird die Beschwerde als unbegründet abgewiesen.

B)

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

Entscheidungsgründe:

I. Verfahrensgang:

1. Am 05.04.2023 teilte eine betroffene Person, XXXX der Datenschutzbehörde mit, sie habe von der Praxis der Beschwerdeführerin, einer niedergelassenen Fachärztin für Psychiatrie und psychotherapeutische Medizin, eine Terminerinnerung für den 06.02.2023 im Rahmen einer Gruppentextnachricht erhalten, welche an insgesamt 28 Patienten versendet worden sei. Dadurch sei auch ihre Telefonnummer gegenüber den anderen Teilnehmern der Gruppentextnachricht offengelegt worden.

2. Das von der Datenschutzbehörde (in der Folge auch „belangte Behörde“) zunächst eingeleitete amtswegige Prüfverfahren zur GZ D213.2083 stellte diese, da für in der Vergangenheit liegende, bereits abgeschlossene, Rechtsverletzungen keine Feststellungskompetenz bestehe, am 18.07.2023 ein und leitete ein Verwaltungsstrafverfahren ein.

3. Mit Schreiben vom 21.09.2023 forderte die belangte Behörde die Beschwerdeführerin zur Rechtfertigung als Beschuldigte im Verwaltungsstrafverfahren auf.

4. Am 17.10.2023 langte hierzu ein Schriftsatz zur Rechtfertigung der anwaltlich vertretenen Beschwerdeführerin bei der belangten Behörde ein, unter einem verwies die Beschwerdeführerin darin auf ihre bereits (im Administrativverfahren) vor der Datenschutzbehörde erstattete Stellungnahme vom 22.06.2023.

5. Mit dem beim Bundesverwaltungsgericht gegenständlich angefochtenen Straferkenntnis vom 02.11.2023 verhängte die belangte Behörde über die Beschwerdeführerin eine Geldstrafe von EUR 6.000,- (im Falle der Uneinbringlichkeit eine Ersatzfreiheitsstrafe von 336 Stunden) gemäß Art. 83 Abs. 5 lit. a DSGVO iVm § 16 VStG und verpflichtete die Beschwerdeführerin zur Leistung eines Beitrages zu den Kosten des Strafverfahrens (§ 64 VStG) im Ausmaß von 10 Prozent der verhängten Geldstrafe, somit in der Höhe von EUR 600,00.

Der Beschwerdeführerin wurde darin zur Last gelegt, sie habe als datenschutzrechtlich Verantwortliche, am 05.04.2023 (im Folgenden „Tatzeit“), von einem in ihrem Besitz befindlichen Endgerät aus (Praxistelefon – Marke: iPhone), in XXXX durch die Nutzung eines Gruppennachrichtendienstes („iMessage“), unrechtmäßig personenbezogene Daten, darunter besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO (Gesundheitsdaten), im Zuge einer Gruppennachricht zum Zwecke der Terminerinnerung verarbeitet, indem sie die Telefonnummern von 28 Patienten gegenüber unbefugten Dritten im Rahmen der erstellten Gruppe offengelegt hat.

Dadurch sei auch die Information offengelegt worden, dass sich diese betroffenen Personen bei der Beschwerdeführerin in Behandlung befänden und mit der Beschwerdeführerin einen Termin hierfür vereinbart haben. Die unrechtmäßige Verarbeitung sei unter anderem auch auf einen Verstoß gegen die Pflichten der Beschwerdeführerin als Verantwortliche nach Art. 25 Abs. 1 und 2 DSGVO zurückzuführen, weil sie zuvor keine geeigneten technischen und organisatorischen Maßnahmen getroffen habe, die sichergestellt hätten, dass durch die Voreinstellung des Endgerätes nur eine für den jeweiligen Verarbeitungszweck erforderliche Verarbeitung erfolge, um insbesondere die Datenschutzgrundsätze der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und der Integrität der Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO) wirksam umzusetzen (Spruchpunkt I.).

Darüber hinaus habe die Beschwerdeführerin in ihrer Rolle als Verantwortliche seit XXXX bis zumindest 22.06.2023 (Tatzeitraum), innerhalb des Bundesgebietes Österreich, gegen ihre Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 1 DSGVO verstoßen, indem sie kein Verzeichnis aller Verarbeitungstätigkeiten, die im Tatzeitraum ihrer Zuständigkeit unterlagen, in der nach Art. 30 Abs. 3 DSGVO genannten Form geführt habe und daher auf Anfrage der Datenschutzbehörde nicht im Sinne des Art. 30 Abs. 4 DSGVO zur Verfügung stellen habe können (Spruchpunkt II.).

Schließlich habe die Beschwerdeführerin in ihrer Rolle als Verantwortliche im Zeitraum vom 05.04.2023 bis 22.06.2023 innerhalb des Bundesgebietes Österreich gegen ihre Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Datenschutzbehörde gemäß Art. 33 Abs. 1 DSGVO verstoßen, indem sie die oben (unter Punkt I.) dargestellte Verletzung des Schutzes der personenbezogenen Daten der Betroffenen durch die unbefugte Offenlegung ihrer (Gesundheits-)Daten gegenüber Dritten nicht unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung ihr bekannt wurde, der Datenschutzbehörde gemeldet hat (Spruchpunkt III.).

Der Tatvorwurf in Bezug auf den Verstoß gegen die Verpflichtung zur Benennung eines Datenschutzbeauftragten nach Art. 37 Abs. 1 lit. c DSGVO in der Rolle als Verantwortliche nach

Art. 4 Z 7 DSGVO (vorgeworfene Verwaltungsübertretung nach Art. 37 Abs. 1 lit. c iVm Art. 83 Abs. 1 und 4 lit. a DSGVO) wurde gemäß § 45 Abs. 1 Z 2 (erster Fall) VStG eingestellt (Spruchpunkt IV.).

Begründend hielt die belangte Behörde zu Spruchpunkt I. im Wesentlichen fest, es liege eine unrechtmäßige Verarbeitung sensibler Daten von mehreren Betroffenen sowie ein Verstoß gegen mehrere Datenschutzgrundsätze vor, die unter anderem auf die Missachtung der Vorgaben nach Art. 25 Abs. 1 und 2 DSGVO bei der Einrichtung und während des Betriebes des Benachrichtigungssystems zurückzuführen seien. Die Beschwerdeführerin habe dadurch die objektive Tatseite der genannten Tatbestände erfüllt.

Zu Spruchpunkt II. führte die belangte Behörde aus, die Beschwerdeführerin habe kein Verzeichnis aller Verarbeitungstätigkeiten im Sinne von Art. 30 Abs. 1 DSGVO geführt und habe ein solches daher auch nicht vorlegen können.

In Bezug auf Spruchpunkt III. hielt die belangte Behörde fest, es sei zu einem Verstoß gegen die Meldepflicht nach Art. 33 DSGVO gekommen, da die Beschwerdeführerin nicht der Ausnahmeregelung unterliege und sie nicht davon ausgehen konnte, die Sicherheitsverletzung werde voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen. Die objektive Tatseite betreffend Art. 33 Abs. 1 DSGVO sei somit ebenfalls erfüllt.

Da die verfahrensgegenständlichen Tatvorwürfe der Beschwerdeführerin jedenfalls subjektiv vorwerfbar seien, sei die subjektive Tatseite ebenfalls erfüllt.

Zur Einstellung (Spruchpunkt IV.) führte die belangte Behörde aus, dass der Vorwurf hinsichtlich der Verletzung des Art. 37 Abs. 1 lit. c DSGVO spruchgemäß einzustellen gewesen sei, da im vorliegenden Fall keine umfangreiche Verarbeitung besonderer Kategorien von Daten nach Art. 9 Abs. 1 DSGVO habe festgestellt werden können.

Was die Strafzumessung betreffe, so sei als erschwerend gewertet worden, dass die Bedeutung des verwaltungsstrafrechtlich geschützten Rechtsgutes im vorliegenden Fall als sehr hoch zu werten sei, es seien zudem besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO betroffen gewesen.

Mildernd sei zu berücksichtigen gewesen, dass die Beschwerdeführerin keine einschlägigen Vorstrafen aufweise, am Verwaltungsstrafverfahren mitgewirkt, und sich umgehend nach Zustellung der Aufforderung zur Stellungnahme im amtswegigen Prüfverfahren mit der technischen Gestaltung des Benachrichtigungssystems auseinandergesetzt, sich beraten lassen und in der Folge die dementsprechenden Änderungen im Rahmen der Einstellungen vorgenommen habe.

Die verhängte Strafe sei im Hinblick auf den verwirklichten Tatumwert gemessen am Strafraumen sowie unter Berücksichtigung der Einkommens- und Vermögensverhältnisse tat- und schuldangemessen.

6. Die Beschwerdeführerin erhob mit Schriftsatz vom 01.12.2023 Beschwerde gegen das gegenständliche Straferkenntnis, räumte darin zunächst dem Grunde nach die Begehung der ihr von der belangten Behörde im angefochtenen Straferkenntnis zur Last gelegten Verstöße gegen datenschutzrechtliche Bestimmungen ein, nach Ansicht der Beschwerdeführerin hätte die belangte Behörde jedoch – unter Anwendung des § 11 DSG und § 34a VStG – mit einer Verwarnung das Auslangen finden oder zumindest eine (niedrigere), tat- und schuldangemessene, Geldstrafe verhängen müssen.

Gestellt werde somit der Antrag, wonach das Bundesverwaltungsgericht in Stattgabe dieser Beschwerde

- das angefochtene Straferkenntnis der belangten Behörde wegen Rechtswidrigkeit des Inhalts aufheben und das Verfahren zur Einstellung bringen wolle, in eventu
- mit einer Verwarnung, in eventu
- mit einer schuld- und tatangemessen herabgesetzten Geldstrafe das Auslangen finden wolle.

7. Mit Schreiben vom 01.12.2023 legte die belangte Behörde die Beschwerde und den Verwaltungsakt dem Bundesverwaltungsgericht vor, erstattete im Zuge dessen eine Stellungnahme und beantragte, die Beschwerde als unbegründet abzuweisen und die Beschwerdeführerin zur Kostentragung nach § 52 VwGVG zu verpflichten.

8. Das Bundesverwaltungsgericht führte in der gegenständlichen Beschwerdesache am 31.01.2024 eine mündliche Beschwerdeverhandlung durch. Im Rahmen der mündlichen Verhandlung fand eine umfassende Erörterung der Sach- und Rechtslage mit den Verfahrensparteien statt, wobei die Beschwerdeführerin rechtsanwaltlich vertreten war.

II. Das Bundesverwaltungsgericht hat erwogen:

II.1. Feststellungen:

II.1.1. Zur Beschwerdeführerin:

Die Beschwerdeführerin ist Fachärztin für Psychiatrie und psychotherapeutische Medizin und betreibt seit XXXX eine Ordination in XXXX

Die Beschwerdeführerin hat im Zuge der Gründung ihrer Arztpraxis keine rechtlichen Beratungsleistungen durch einen Rechtsanwalt eingeholt, sondern sich lediglich unter

Kollegen erkundigt. Ob und welchen rechtlichen Rat die Beschwerdeführerin bei der Ärztekammer gesucht oder eingeholt hat, kann nicht festgestellt werden.

II.1.2. Zum Versand der inkriminierten Terminerinnerungen an Patienten im Wege des Messenger-Dienstes „iMessage“:

Seit dem Jahreswechsel 2022/2023 hat die Beschwerdeführerin in Form von Text-Nachrichten mittels des für ihre Praxis genutzten Mobiltelefons vom Typ Apple iPhone Terminerinnerungen an ihre Patienten versandt.

Die jeweiligen Nachrichten wurden von der Ordinationsassistentin der Beschwerdeführerin manuell versandt und nicht automatisch generiert.

Am 05.04.2023 versandte die Ordinationsassistentin der Beschwerdeführerin die inkriminierte Nachricht zur Erinnerung an Termine am 06.04.2023, dies in Form einer Gruppentextnachricht an insgesamt 27 Personen als Empfänger.

Die gegenständliche Gruppentextnachricht an 27 Patienten stellte sich graphisch dar wie folgt:

Für den Fall, dass die Empfänger der Nachricht die Schaltfläche mit der Beschriftung „28 People“ betätigten, gelangten diese zu einer Ansicht, in der ihnen die Telefonnummern sämtlicher 28 Empfänger angezeigt wurden, da die Nachricht in Form einer Gruppen-Nachricht erstellt und verschickt wurde.

Dadurch wurden die Telefonnummern sämtlicher 28 Empfänger jeweils allen anderen Empfängern (Teilnehmern der Gruppennachricht) offengelegt.

Darüber hinaus enthielt die gegenständliche Gruppennachricht keine weiteren personenbezogenen Daten der Empfänger und eingeladenen Patienten.

II.1.3. Zur Änderung der Einstellungen durch die Beschwerdeführerin:

Die Beschwerdeführerin hat sich in Reaktion auf den Vorfall vom 05.04.2023 technisch beraten lassen, die Einstellungen an dem von ihr genutzten Endgerät angepasst, um das Versenden von Nachrichten an iPhone-Nutzer per iMessage zu unterbinden und einen Versand im Wege von konventionellen Textnachrichten (SMS) sicherzustellen bzw. ähnliche Vorfälle zu verhindern.

II.1.4. Zum (fehlenden) Verarbeitungsverzeichnis:

Die Beschwerdeführerin hat, seit 01.12.2022 bis zu ihrer Stellungnahme im amtswegigen Prüfverfahren vor der Datenschutzbehörde vom 22.06.2023, kein Verzeichnis über ihre Verarbeitungstätigkeiten im Rahmen ihrer ärztlichen Berufsausübung geführt.

Am 07.07.2023 übermittelte die Beschwerdeführerin der belangten Behörde ein Verarbeitungsverzeichnis, das sie nach der Aufforderung zur Stellungnahme durch die Datenschutzbehörde zu einem nicht näher bestimmbareren Zeitpunkt erstellt hatte.

II.1.5. Zur unterbliebenen Meldung des Vorfalles als Sicherheitsverletzung bei der belangten Behörde:

Die Beschwerdeführerin brachte in Reaktion auf den Vorfall vom 05.04.2023 keine Meldung bei der belangten Behörde im Sinne von Art. 33 DSGVO ein, sie informierte die Datenschutzbehörde auch sonst nicht über den Vorfall vom 05.04.2023.

II.1.6. Zur Einstellung des amtswegigen Prüfverfahrens:

Das von der belangten Behörde zunächst eingeleitete amtswegige Prüfverfahren zur GZ D213.2083 stellte diese am 18.07.2023 ein und leitete die belangte Behörde für die in der Vergangenheit liegenden Verstöße das gegenständliche Verwaltungsstrafverfahren ein.

II.1.7. Zu den Einkommens- und Vermögensverhältnissen sowie Sorgepflichten der Beschwerdeführerin:

Die Beschwerdeführerin erzielt ein durchschnittliches monatliches Nettoeinkommen in Höhe von zumindest 2.900,00 Euro. Die Beschwerdeführerin ist sorgepflichtig für zwei minderjährige Kinder sowie ein studierendes Kind. Die Beschwerdeführerin ist Hälfteigentümerin eines Einfamilienhauses, wobei hierfür eine Kreditverbindlichkeit in der Höhe von EUR 280.000,00 besteht.

II.2. Beweiswürdigung:

II.2.1. Zu II.1.1. (Zur Beschwerdeführerin):

Die Feststellungen zur Beschwerdeführerin konnten aufgrund der Angaben der Beschwerdeführerin vor dem Bundesverwaltungsgericht getroffen werden und waren insofern unstrittig.

Dass die Beschwerdeführerin im Zuge der Gründung ihrer Arztpraxis keinerlei rechtlichen Beratungsleistungen eines Rechtsanwaltes in Anspruch genommen hat, ergibt sich aus der diesbezüglich klaren und eindeutigen Aussage der Beschwerdeführerin vor dem Bundesverwaltungsgericht. Die Angaben der Beschwerdeführerin, wonach eine Erkundigung bei der Ärztekammer keinerlei konkreten Hinweise auf datenschutzrechtliche Verpflichtungen im Zusammenhang mit der Führung einer Facharztpraxis ergeben habe, erscheinen bei verständiger Betrachtung aus Sicht des erkennenden Senates nicht schlüssig nachvollziehbar, vielmehr wäre aus Sicht des Bundesverwaltungsgerichtes jedenfalls zu erwarten, dass die Ärztekammer ihren Mitgliedern in Bezug auf die Gründung einer Praxis auf Anfrage hin jedenfalls Informationen zu den wesentlichen rechtlichen Rahmenbedingungen, auch und gerade mit Blick auf datenschutzrechtliche Erfordernisse, zur Verfügung stellt. Dem diesbezüglichen Vorbringen der Beschwerdeführerin war daher aus Sicht des erkennenden Senates die Glaubhaftigkeit zu versagen.

II.2.2. Zu II.1.2. Zum Versand von Terminerinnerungen an Patienten der Beschwerdeführerin:

Dass die Ordinationsassistentin seit dem Jahreswechsel 2022/2023 Terminerinnerungen in Form einer Gruppen-Nachricht mittels des Praxistelefons an Patienten manuell versandte, folgt aus den Ausführungen der Beschwerdeführerin hierzu vor dem Bundesverwaltungsgericht; diese decken sich mit den schriftlichen Stellungnahmen vom 22.06.2023 sowie vom 17.10.2023 im verwaltungsbehördlichen Verfahren.

Die Feststellung zum Versand der Gruppentextnachricht am 05.04.2023 konnte auf Basis der Datenschutzbeschwerde, welche am 05.04.2023 bei der belangten Behörde einlangte, getroffen werden und wurden diese von der Beschwerdeführerin auch zu keinem Zeitpunkt vor dem Bundesverwaltungsgericht bestritten. Die Beschwerdeführerin räumt im Rahmen

ihres Beschwerdeschriftsatzes vom 01.12.2023 selbst ein, die Verstöße gegen datenschutzrechtliche Bestimmungen seien zu Recht festgestellt worden.

II.2.3. Zu II.1.3. Änderung der (Vor-)Einstellungen des für den Versand von Terminerinnerungsnachrichten genutzten Endgerätes durch die Beschwerdeführerin:

Die Feststellungen zur vorgenommenen Einstellungsänderung konnten auf Basis der glaubhaften Angaben der Beschwerdeführerin im Verwaltungsverfahren erfolgen. So hat sie mehrfach gleichbleibend vorgebracht, sie habe sich in Reaktion auf den Vorfall vom 05.04.2023 technisch beraten lassen und die Einstellungen entsprechend angepasst, um den Versand der inkriminierten Gruppentextnachrichten künftig zu unterbinden.

II.2.4. Zu II.1.4. Zum fehlenden Verarbeitungsverzeichnis:

Der Umstand, wonach die Beschwerdeführerin seit Eröffnung ihrer Ordination, jedenfalls bis zur Stellungnahme im amtswegigen Prüfverfahren vor der Datenschutzbehörde am 22.06.2023, kein Verzeichnis über ihre Verarbeitungstätigkeiten geführt hatte, folgt aus den hierzu schlüssigen Angaben der Beschwerdeführerin im verwaltungsbehördlichen Verfahren, dieser Umstand wurde von der Beschwerdeführerin im Verfahren vor dem Bundesverwaltungsgericht auch nicht in Abrede gestellt.

II.2.5. Zu II.1.5. Zum Unterbleiben der Meldung des Vorfalles an die Datenschutzbehörde:

Dass die Beschwerdeführerin in Reaktion auf den Vorfall vom 05.04.2023 keine Meldung an die belangte Behörde vorgenommen hat, wurde von der Beschwerdeführerin selbst zu keinem Zeitpunkt in Abrede gestellt bzw. wurde dieser Umstand vor dem Bundesverwaltungsgericht von **der Beschwerdeführerin** erneut eingeräumt.

II.2.6. Zu II.1.6. (Zur Einstellung des amtswegigen Prüfverfahrens):

Dass die belangte Behörde das zunächst eingeleitete amtswegige Prüfverfahren zur GZ D213.2083 am 18.07.2023 eingestellt und in der Folge das gegenständliche Verwaltungsstrafverfahren eingeleitet hat, folgt aus dem unbedenklichen Verwaltungsakt, insbesondere aus der Mitteilung der belangten Behörde vom 18.07.2023.

II.2.7. Zu II.1.7. Zu den Einkommens- und Vermögensverhältnissen sowie den Sorgepflichten der Beschwerdeführerin:

Da zu den aktuellen Einkommensverhältnissen von der Beschwerdeführerin keine unbedenklichen Belege (Steuerbescheid u.ä.) vorgelegt werden konnten, geht das Bundesverwaltungsgericht zumindest von denselben Einkommensverhältnissen aus, die auch von der belangten Behörde herangezogen wurden. Die im Nachgang der mündlichen

Verhandlung in Vorlage gebrachten Schätzungen zu den Einkommensverhältnissen aus der Tätigkeit als niedergelassene Fachärztin erscheinen nicht schlüssig und nachvollziehbar, dies insbesondere vor dem Hintergrund, dass die Beschwerdeführerin dazu befragt in der mündlichen Verhandlung angab, monatlich von ihrem Geschäftskonto 4.000,00 bis 5.000,00 Euro zum privaten Gebrauch zu entnehmen.

Im Übrigen ergeben sich die getroffenen Feststellungen zu den Vermögensverhältnissen und Sorgepflichten anhand der diesbezüglichen Angaben der Beschwerdeführerin vor dem Bundesverwaltungsgericht, wobei diese mit den im verwaltungsbehördlichen Verfahren hierzu getätigten Angaben der Beschwerdeführerin korrespondieren.

II.3. Rechtliche Beurteilung:

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

Da es sich beim Beschwerdegegenstand um einen Bescheid der Datenschutzbehörde handelt, liegt gemäß § 27 DSG Senatszuständigkeit vor.

II.3.1. Zu Spruchpunkt A) – Teilweise Stattgabe der Beschwerde:

Anzuwendendes Recht:

Die hier maßgebenden Bestimmungen und Erwägungsgründe der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ABl. L 119 vom 04.05.2016, im Folgenden: DSGVO, lauten auszugsweise samt Überschrift:

„Artikel 1

Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

(3) ...

Artikel 4

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

(1) „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

(2) „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

...

(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;

(9) „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

(10) „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

(11) „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

(12) „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

...

(15) „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

...

(18) „Unternehmen“ eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;

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“).

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Artikel 58

Befugnisse

(1) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Untersuchungsbefugnisse, die es ihr gestatten,

- a) den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind,
- b) Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen,
- c) eine Überprüfung der nach Artikel 42 Absatz 7 erteilten Zertifizierungen durchzuführen,
- d) den Verantwortlichen oder den Auftragsverarbeiter auf einen vermeintlichen Verstoß gegen diese Verordnung hinzuweisen,
- e) von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten,
- f) gemäß dem Verfahrensrecht der Union oder dem Verfahrensrecht des Mitgliedstaats Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten.

(2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,

- a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,
- b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat,
- c) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen,
- d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,
- e) den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person entsprechend zu benachrichtigen,
- f) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,
- g) die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß den Artikeln 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Artikel 17 Absatz 2 und Artikel 19 offengelegt wurden, über solche Maßnahmen anzuordnen,
- h) eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,

i) eine Geldbuße gemäß Artikel 83 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls,

j) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.

(3) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Genehmigungsbefugnisse und beratenden Befugnisse, die es ihr gestatten,

a) gemäß dem Verfahren der vorherigen Konsultation nach Artikel 36 den Verantwortlichen zu beraten,

b) zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an das nationale Parlament, die Regierung des Mitgliedstaats oder im Einklang mit dem Recht des Mitgliedstaats an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten,

c) die Verarbeitung gemäß Artikel 36 Absatz 5 zu genehmigen, falls im Recht des Mitgliedstaats eine derartige vorherige Genehmigung verlangt wird,

d) eine Stellungnahme abzugeben und Entwürfe von Verhaltensregeln gemäß Artikel 40 Absatz 5 zu billigen,

e) Zertifizierungsstellen gemäß Artikel 43 zu akkreditieren,

f) im Einklang mit Artikel 42 Absatz 5 Zertifizierungen zu erteilen und Kriterien für die Zertifizierung zu billigen,

g) Standarddatenschutzklauseln nach Artikel 28 Absatz 8 und Artikel 46 Absatz 2 Buchstabe d festzulegen,

h) Vertragsklauseln gemäß Artikel 46 Absatz 3 Buchstabe a zu genehmigen,

i) Verwaltungsvereinbarungen gemäß Artikel 46 Absatz 3 Buchstabe b zu genehmigen

j) verbindliche interne Vorschriften gemäß Artikel 47 zu genehmigen.

(4) Die Ausübung der der Aufsichtsbehörde gemäß diesem Artikel übertragenen Befugnisse erfolgt vorbehaltlich geeigneter Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta.

(5) Jeder Mitgliedstaat sieht durch Rechtsvorschriften vor, dass seine Aufsichtsbehörde befugt ist, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die Bestimmungen dieser Verordnung durchzusetzen.

(6) Jeder Mitgliedstaat kann durch Rechtsvorschriften vorsehen, dass seine Aufsichtsbehörde neben den in den Absätzen 1, 2 und 3 aufgeführten Befugnissen über zusätzliche Befugnisse verfügt. Die Ausübung dieser Befugnisse darf nicht die effektive Durchführung des Kapitels VII beeinträchtigen.

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 abzuwehren 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;
- c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;
- d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;
- e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels 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.

(7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

(8) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

(9) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.“

In den Erwägungsgründen 9, 10, 11, 13, 74, 85, 129, 148 und 150 der DSGVO heißt es:

„(9) ... Unterschiede beim Schutzniveau für die Rechte und Freiheiten von natürlichen Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten in den Mitgliedstaaten, vor allem beim Recht auf Schutz dieser Daten, können den unionsweiten freien Verkehr solcher Daten behindern. Diese Unterschiede im Schutzniveau können daher ein Hemmnis für die unionsweite Ausübung von Wirtschaftstätigkeiten darstellen, den Wettbewerb verzerren und die Behörden an der Erfüllung der ihnen nach dem Unionsrecht obliegenden Pflichten hindern. ...

(10) Um ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden. Hinsichtlich der Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, sollten die Mitgliedstaaten die Möglichkeit haben, nationale Bestimmungen, mit denen die Anwendung der Vorschriften dieser Verordnung genauer festgelegt wird, beizubehalten oder einzuführen. ... Diese Verordnung bietet den Mitgliedstaaten zudem einen Spielraum für die Spezifizierung ihrer Vorschriften, auch für die Verarbeitung besonderer Kategorien von personenbezogenen Daten ... Diesbezüglich schließt diese Verordnung nicht Rechtsvorschriften der Mitgliedstaaten aus, in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

(11) Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert die Stärkung und präzise Festlegung der Rechte der betroffenen Personen sowie eine Verschärfung der Verpflichtungen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden, ebenso wie – in den Mitgliedstaaten – gleiche Befugnisse bei der Überwachung und Gewährleistung

der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung.

...

(13) Damit in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, beseitigt werden, ist eine Verordnung erforderlich, die für die Wirtschaftsteilnehmer einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen Rechtssicherheit und Transparenz schafft, natürliche Personen in allen Mitgliedstaaten mit demselben Niveau an durchsetzbaren Rechten ausstattet, dieselben Pflichten und Zuständigkeiten für die Verantwortlichen und Auftragsverarbeiter vorsieht und eine gleichmäßige Kontrolle der Verarbeitung personenbezogener Daten und gleichwertige Sanktionen in allen Mitgliedstaaten sowie eine wirksame Zusammenarbeit zwischen den Aufsichtsbehörden der einzelnen Mitgliedstaaten gewährleistet. ...

...

(74) Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind. Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen.

...

(85) Eine Verletzung des Schutzes personenbezogener Daten kann — wenn nicht rechtzeitig und angemessen reagiert wird — einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person. Deshalb sollte der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, unterrichten, es sei denn, der Verantwortliche kann im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Falls diese

Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen, und die Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.

...

(129) Um die einheitliche Überwachung und Durchsetzung dieser Verordnung in der gesamten Union sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und wirksamen Befugnisse haben, darunter ... Untersuchungsbefugnisse, Abhilfebefugnisse und Sanktionsbefugnisse ... Insbesondere sollte jede Maßnahme im Hinblick auf die Gewährleistung der Einhaltung dieser Verordnung geeignet, erforderlich und verhältnismäßig sein, wobei die Umstände des jeweiligen Einzelfalls zu berücksichtigen sind, das Recht einer jeden Person, gehört zu werden, bevor eine individuelle Maßnahme getroffen wird, die nachteilige Auswirkungen auf diese Person hätte, zu achten ist und überflüssige Kosten und übermäßige Unannehmlichkeiten für die Betroffenen zu vermeiden sind. Untersuchungsbefugnisse im Hinblick auf den Zugang zu Räumlichkeiten sollten im Einklang mit besonderen Anforderungen im Verfahrensrecht der Mitgliedstaaten ausgeübt werden, wie etwa dem Erfordernis einer vorherigen richterlichen Genehmigung. Jede rechtsverbindliche Maßnahme der Aufsichtsbehörde sollte schriftlich erlassen werden und sie sollte klar und eindeutig sein; die Aufsichtsbehörde, die die Maßnahme erlassen hat, und das Datum, an dem die Maßnahme erlassen wurde, sollten angegeben werden und die Maßnahme sollte vom Leiter oder von einem von ihm bevollmächtigten Mitglied der Aufsichtsbehörde unterschrieben sein und eine Begründung für die Maßnahme sowie einen Hinweis auf das Recht auf einen wirksamen Rechtsbehelf enthalten. Dies sollte zusätzliche Anforderungen nach dem Verfahrensrecht der Mitgliedstaaten nicht ausschließen. ...

...

(148) Im Interesse einer konsequenteren Durchsetzung der Vorschriften dieser Verordnung sollten bei Verstößen gegen diese Verordnung zusätzlich zu den geeigneten Maßnahmen, die die Aufsichtsbehörde gemäß dieser Verordnung verhängt, oder an Stelle solcher Maßnahmen Sanktionen einschließlich Geldbußen verhängt werden. Im Falle eines geringfügigeren Verstoßes oder falls voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, kann anstelle einer Geldbuße eine Verwarnung erteilt werden. Folgendem sollte jedoch gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes, dem vorsätzlichen Charakter des Verstoßes, den Maßnahmen zur Minderung des entstandenen Schadens, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, der Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, der Einhaltung der gegen den Verantwortlichen oder Auftragsverarbeiter angeordneten Maßnahmen, der Einhaltung von Verhaltensregeln und jedem anderen erschwerenden oder mildernden Umstand. Für die Verhängung von Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des

Unionsrechts und der Charta, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.

(150) Um die verwaltungsrechtlichen Sanktionen bei Verstößen gegen diese Verordnung zu vereinheitlichen und ihnen mehr Wirkung zu verleihen, sollte jede Aufsichtsbehörde befugt sein, Geldbußen zu verhängen. In dieser Verordnung sollten die Verstöße sowie die Obergrenze der entsprechenden Geldbußen und die Kriterien für ihre Festsetzung genannt werden, wobei diese Geldbußen von der zuständigen Aufsichtsbehörde in jedem Einzelfall unter Berücksichtigung aller besonderen Umstände und insbesondere der Art, Schwere und Dauer des Verstoßes und seiner Folgen sowie der Maßnahmen, die ergriffen worden sind, um die Einhaltung der aus dieser Verordnung erwachsenden Verpflichtungen zu gewährleisten und die Folgen des Verstoßes abzuwenden oder abzumildern, festzusetzen sind. Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff ‚Unternehmen‘ im Sinne der Artikel 101 und 102 AEUV verstanden werden. ...“

II.3.2. Zum Beschwerdevorbringen:

Die Beschwerdeführerin beantragt im Rahmen ihrer Beschwerde unter näherer Begründung, worauf nachfolgend im Einzelnen einzugehen sein wird, das Bundesverwaltungsgericht wolle

- das angefochtene Straferkenntnis der belangten Behörde wegen Rechtswidrigkeit des Inhalts aufheben und das Verfahren zur Einstellung bringen, *in eventu*
- mit einer Verwarnung, *in eventu*
- mit einer schuld- und tatangemessen herabgesetzten Geldstrafe das Auslangen finden.

Im Rahmen der mündlichen Beschwerdeverhandlung präzisiert die Beschwerdeführerin ihr Beschwerdevorbringen – auf Nachfrage des Senatsvorsitzenden hinsichtlich des Erklärungswertes des Beschwerdeschriftsatzes – dahingehend, dass sich der Umfang der Anfechtung hinsichtlich der Spruchpunkte I. und II. lediglich auf das Ausmaß der verhängten Strafe bezieht, in Bezug auf Spruchpunkt III. jedoch auch auf die Feststellung der Verwirklichung des vorgeworfenen Verwaltungsstraftatbestandes dem Grunde nach erstreckt.

II.3.3. Allgemeines zur Verhängung von Geldbußen nach Art. 83 DSGVO:

II.3.3.1. Mit der Datenschutz-Grundverordnung („DSGVO“), die seit dem 25. Mai 2018 anwendbar ist, hat die EU eine umfassende Reform der Datenschutzvorschriften in Europa vollendet. Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Die Verordnung stützt sich auf mehrere Schlüsselkomponenten, zu denen unter anderem stärkere Durchsetzungsbefugnisse der Aufsichtsbehörden gehören. Die DSGVO sieht als Neuerung deutlich höhere Geldbußen sowie eine Harmonisierung der Geldbußen zwischen den Mitgliedstaaten vor. Verantwortliche und Auftragsverarbeiter haben

mehr als zuvor Sorge dafür zu tragen, dass die personenbezogenen Daten natürlicher Personen wirksam geschützt werden. Die Aufsichtsbehörden sind befugt sicherzustellen, dass die Grundsätze der DSGVO sowie die Rechte der betroffenen Personen gemäß dem Wortlaut und dem Geist der DSGVO gewahrt werden. Die DSGVO schreibt vor, dass der Betrag der Geldbuße in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein muss (Artikel 83 Abs. 1 DSGVO). Darüber hinaus haben die Aufsichtsbehörden bei der Festsetzung des Betrags der Geldbuße eine Liste von Umständen zu berücksichtigen, die sich auf Merkmale des Verstoßes (seine Schwere) oder das Verhalten des den Verstoß Begehenden beziehen (Art. 83 Abs. 2 DSGVO). Die Quantifizierung des Betrags der Geldbuße beruht daher auf einer konkreten Bewertung, die in jedem Einzelfall unter Berücksichtigung der in der DSGVO enthaltenen Parameter vorgenommen wird. Eine Mindestgeldbuße sieht die DSGVO für Verhaltensweisen, die gegen Datenschutzvorschriften verstoßen, nicht vor. Vielmehr sieht die DSGVO in ihrem Artikel 83 Absätze 4 bis 6, in denen verschiedene Verhaltensweisen zusammengefasst werden, lediglich Höchstbeträge vor. Eine Geldbuße kann letztlich nur durch Abwägung aller in Artikel 83 Abs. 2 lit. a bis j DSGVO ausdrücklich genannten Umstände, die für den Fall relevant sind, und anderer relevanter Anhaltspunkte berechnet werden, auch wenn sie in den genannten Bestimmungen nicht ausdrücklich aufgeführt sind (da Art. 83 Abs. 2 lit. k DSGVO verlangt, dass jeglichen anderen anwendbaren Umständen gebührend Rechnung getragen wird). Schließlich muss der endgültige Betrag der Geldbuße, der sich aus dieser Prüfung ergibt, in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein (Art. 83 Abs. 1 DSGVO). Jede verhängte Geldbuße muss all diesen Parametern ausreichend Rechnung tragen und darf gleichzeitig das in Art. 83 Abs. 4 bis 6 DSGVO vorgesehene gesetzliche Höchstmaß nicht überschreiten (vgl. zu alledem die Leitlinien 04/2022 des Europäischen Datenschutzausschusses für die Berechnung von Geldbußen im Sinne der DSGVO, Version 2.1, Angenommen am 24.05.2023 [im Folgenden: EDSA Leitlinien 2023 zu Art. 83 DSGVO], Rz. 1 – 16).

II.3.3.2. In seiner jüngst ergangenen Rechtsprechung zu Art. 83 DSGVO hält der Europäische Gerichtshof (EuGH) zur Verhängung von Geldbußen durch nationale Aufsichtsbehörden die im folgenden dargestellten Grundsätze fest.

Im Urteil vom 05.12.2023 in der Rechtssache C-807/21 [Deutsche Wohnen SE] führt der EuGH aus wie folgt [Hervorhebungen durch das Bundesverwaltungsgericht]:

„38 Zur Beantwortung der ersten Vorlagefrage ist zunächst festzustellen, dass sich die in der DSGVO vorgesehenen Grundsätze, Verbote und Pflichten insbesondere an „Verantwortliche“ richten. Deren Verantwortung und Haftung erstreckt sich nach den Ausführungen im 74. Erwägungsgrund der DSGVO auf jedwede Verarbeitung

personenbezogener Daten, die durch sie oder in ihrem Namen erfolgt. In diesem Rahmen müssen sie nicht nur geeignete und wirksame Maßnahmen treffen, sondern sie müssen auch nachweisen können, dass ihre Verarbeitungstätigkeiten im Einklang mit der DSGVO stehen und die Maßnahmen, die sie ergriffen haben, um diesen Einklang sicherzustellen, auch wirksam sind. Diese Haftung ist es, die bei einem der in Art. 83 Abs. 4 bis 6 DSGVO genannten Verstöße die Grundlage dafür bildet, nach Art. 83 DSGVO eine Geldbuße gegen den Verantwortlichen zu verhängen.

39 In Art. 4 Nr. 7 DSGVO ist der Begriff „Verantwortlicher“ weit definiert als die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

40 Das Ziel dieser weiten Definition des Art. 4 Nr. 7 DSGVO – die ausdrücklich auch juristische Personen einschließt – besteht im Einklang mit dem Ziel der DSGVO darin, einen wirksamen Schutz der Grundfreiheiten und Grundrechte natürlicher Personen und insbesondere ein hohes Schutzniveau für das Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten zu gewährleisten (vgl. in diesem Sinne Urteile vom 29. Juli 2019, Fashion ID, C-40/17, EU:C:2019:629, Rn. 66, und vom 28. April 2022, Meta Platforms Ireland, C-319/20, EU:C:2022:322, Rn. 73 sowie die dort angeführte Rechtsprechung).

41 Des Weiteren hat der Gerichtshof bereits entschieden, dass eine natürliche oder juristische Person, die aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt, als Verantwortlicher angesehen werden kann (vgl. in diesem Sinne Urteil vom 10. Juli 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, Rn. 68).

42 Somit ergibt sich aus dem Wortlaut und dem Zweck von Art. 4 Nr. 7 DSGVO, dass der Unionsgesetzgeber bei der Bestimmung der Haftung nach der DSGVO nicht zwischen natürlichen und juristischen Personen unterschieden hat, da die einzige Voraussetzung für diese Haftung darin besteht, dass diese Personen allein oder zusammen mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.

43 Vorbehaltlich der Bestimmungen von Art. 83 Abs. 7 DSGVO betreffend Behörden und öffentliche Stellen haftet daher jede Person, die diese Voraussetzung erfüllt – unabhängig davon, ob es sich um eine natürliche oder juristische Person, eine Behörde, Einrichtung oder andere Stelle handelt – u. a. für jeden in Art. 83 Abs. 4 bis 6 der DSGVO genannten Verstoß, der von ihr selbst oder in ihrem Namen begangen wurde.

...

45 Sodann legt Art. 58 Abs. 2 DSGVO die Befugnisse der Aufsichtsbehörden zum Erlass von Abhilfemaßnahmen genau fest, ohne auf das Recht der Mitgliedstaaten zu verweisen oder den Mitgliedstaaten einen Ermessensspielraum einzuräumen. Zum einen zielen diese Befugnisse, zu denen gemäß Art. 58 Abs. 2 Buchst. i DSGVO die Befugnis zur Verhängung von Geldbußen gehört, auf den Verantwortlichen ab, und zum anderen kann ein solcher Verantwortlicher, wie aus Rn. 39 des vorliegenden Urteils hervorgeht, sowohl eine natürliche als auch eine juristische Person sein. Die materiellen Voraussetzungen, die eine Aufsichtsbehörde bei der Verhängung einer solchen Geldbuße zu beachten hat, sind in Art. 83 Abs. 1 bis 6 DSGVO genau und ohne Ermessensspielraum für die Mitgliedstaaten aufgeführt.

...

47 Zwar ergibt sich aus Art. 58 Abs. 4 und Art. 83 Abs. 8 DSGVO im Licht des 129. Erwägungsgrundes der DSGVO, dass die Ausübung der Befugnisse, über die die Aufsichtsbehörde gemäß diesen Artikeln verfügt, angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen muss.

48 Die Tatsache, dass die DSGVO den Mitgliedstaaten somit die Möglichkeit einräumt, Anforderungen an das von den Aufsichtsbehörden anzuwendende Verfahren bei der Verhängung einer Geldbuße vorzusehen, bedeutet jedoch keineswegs, dass sie auch befugt wären, über diese verfahrensrechtlichen Anforderungen hinaus materielle Voraussetzungen vorzusehen, die zu den in Art. 83 Abs. 1 bis 6 DSGVO geregelten hinzutreten. Des Weiteren wird durch den Umstand, dass der Unionsgesetzgeber eigens und ausdrücklich diese Möglichkeit vorgesehen hat, aber nicht diejenige, solche zusätzlichen materiellen Voraussetzungen festzulegen, bestätigt, dass er den Mitgliedstaaten insoweit keinen Ermessensspielraum gelassen hat. Für diese materiellen Voraussetzungen gilt daher ausschließlich das Unionsrecht.

49 Die vorstehende wörtliche Auslegung von Art. 58 Abs. 2 und Art. 83 Abs. 1 bis 6 DSGVO wird durch den Zweck der DSGVO bestätigt.

50 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. In den Erwägungsgründen 11

und 129 der DSGVO wird außerdem das Erfordernis betont, zur Sicherstellung einer einheitlichen Anwendung der DSGVO sicherzustellen, dass die Aufsichtsbehörden über gleiche Befugnisse bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie über gleiche Sanktionen im Fall von Verstößen gegen die DSGVO verfügen.

...

52 Nach Art. 288 Abs. 2 AEUV ist eine Unionsverordnung in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat, so dass es, sofern nichts anderes bestimmt ist, ausgeschlossen ist, dass die Mitgliedstaaten innerstaatliche Vorschriften erlassen, die die Tragweite einer solchen Verordnung beeinträchtigen. Außerdem dürfen die Mitgliedstaaten aufgrund der ihnen aus dem AEU-Vertrag obliegenden Verpflichtungen die unmittelbare Geltung, die den Verordnungen innewohnt, nicht vereiteln. Insbesondere dürfen sie keine Handlung vornehmen, durch die die unionsrechtliche Natur einer Rechtsvorschrift und die sich daraus ergebenden Wirkungen den Einzelnen verborgen würden (Urteil vom 15. November 2012, Al-Aqsa/Rat und Niederlande/Al-Aqsa, C-539/10 P und C-550/10 P, EU:C:2012:711, Rn. 86 und 87 sowie die dort angeführte Rechtsprechung).

...

61 Mit seiner zweiten Frage, die für den Fall gestellt wird, dass die erste Frage bejaht wird, möchte das vorliegende Gericht im Wesentlichen wissen, ob 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.

62 Insoweit ist darauf hinzuweisen, dass nach Art. 83 Abs. 1 DSGVO Geldbußen wirksam, verhältnismäßig und abschreckend sein müssen. Dagegen enthält Art. 83 DSGVO keine ausdrückliche Klarstellung, dass die in seinen Abs. 4 bis 6 genannten Verstöße nur dann mit einer solchen Geldbuße geahndet werden können, wenn sie vorsätzlich oder zumindest fahrlässig begangen wurden.

...

65 Wie in den Rn. 45 und 48 des vorliegenden Urteils ausgeführt, gilt für die materiellen Voraussetzungen, die eine Aufsichtsbehörde bei der Verhängung einer Geldbuße gegen einen Verantwortlichen zu beachten hat, ausschließlich das Unionsrecht. Diese Voraussetzungen sind in Art. 83 Abs. 1 bis 6 DSGVO genau festgelegt und lassen den Mitgliedstaaten keinen

Ermessensspielraum (vgl. auch Urteil vom 5. Dezember 2023, Nacionalinis visuomenės sveikatos centras, C-683/21, EU:C:2023:XXX, Rn. 64 bis 70).

66 Zu diesen Voraussetzungen ist festzustellen, dass Art. 83 Abs. 2 DSGVO die Kriterien anführt, die die Aufsichtsbehörde bei der Verhängung einer Geldbuße gegen den Verantwortlichen berücksichtigt. Zu diesen Kriterien gehört nach Buchst. b dieser Bestimmung die „Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes“. Dagegen deutet keines der in der genannten Bestimmung aufgeführten Kriterien auf eine Möglichkeit hin, den Verantwortlichen unabhängig von seinem Verschulden haftbar zu machen.

67 Zudem ist der zweite Absatz von Art. 83 DSGVO in Verbindung mit seinem dritten Absatz zu lesen, der bestimmt, welche Folgen bei der Kumulierung von Verstößen gegen die DSGVO eintreten, und wie folgt lautet: „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.“

68 Aus dem Wortlaut von Art. 83 Abs. 2 DSGVO ergibt sich somit, dass nur Verstöße gegen die Bestimmungen der DSGVO, die der Verantwortliche schuldhaft, d. h. vorsätzlich oder fahrlässig, begeht, zur Verhängung einer Geldbuße gegen ihn nach diesem Artikel führen können.

69 Die allgemeine Systematik und der Zweck der DSGVO bestätigen diese Lesart.

70 Zum einen hat der Unionsgesetzgeber ein Sanktionssystem vorgesehen, das es den Aufsichtsbehörden ermöglicht, je nach den Umständen des Einzelfalls die geeignetste Sanktion zu verhängen.

71 Art. 58 Abs. 2 Buchst. i der DSGVO bestimmt nämlich, dass die Aufsichtsbehörden befugt sind, eine Geldbuße gemäß Art. 83 DSGVO „zusätzlich zu oder anstelle von“ anderen in Art. 58 Abs. 2 genannten Abhilfebefugnissen wie die Befugnis zur Erteilung von Warnungen, Verwarnungen oder Anweisungen zu verhängen. Ebenso heißt es im 148. Erwägungsgrund dieser Verordnung u. a., dass es den Aufsichtsbehörden gestattet ist, im Fall eines geringfügigeren Verstoßes oder falls die voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, von der Verhängung einer Geldbuße abzusehen und stattdessen eine Verwarnung zu erteilen.

72 Zum anderen haben die Bestimmungen der DSGVO, wie in Rn. 50 des vorliegenden Urteils ausgeführt, u. a. die Ziele, 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. Zur Sicherstellung einer einheitlichen Anwendung der DSGVO müssen die Aufsichtsbehörden zudem über gleiche Befugnisse bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten verfügen, so dass sie im Fall von Verstößen gegen die DSGVO die gleichen Sanktionen verhängen können.

73 Ein Sanktionssystem, das es ermöglicht, eine Geldbuße gemäß Art. 83 DSGVO zu verhängen, wenn die besonderen Umstände des Einzelfalls dies rechtfertigen, schafft für Verantwortliche und Auftragsverarbeiter einen Anreiz, der DSGVO nachzukommen. Geldbußen tragen durch ihre abschreckende Wirkung zu einem stärkeren Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten bei. Sie sind daher ein Schlüsselement, um die Wahrung der Rechte dieser Personen zu gewährleisten, und stehen im Einklang mit dem Ziel der DSGVO, ein hohes Schutzniveau für solche Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten.

74 Der Unionsgesetzgeber hat es jedoch nicht für erforderlich gehalten, zur Gewährleistung eines solchen hohen Schutzniveaus vorzusehen, dass Geldbußen verschuldensunabhängig verhängt werden. In Anbetracht dessen, dass die DSGVO auf ein gleichwertiges und einheitliches Schutzniveau abzielt und hierfür in der gesamten Union gleichmäßig angewandt werden muss, liefe es diesem Ziel zuwider, den Mitgliedstaaten zu gestatten, eine solche Regelung für die Verhängung einer Geldbuße nach Art. 83 DSGVO vorzusehen. Eine solche Wahlfreiheit wäre zudem geeignet, den Wettbewerb zwischen den Wirtschaftsteilnehmern in der Union zu verfälschen, was den vom Unionsgesetzgeber u. a. in den Erwägungsgründen 9 und 13 der DSGVO dargestellten Zielen zuwiderliefe.

75 Demnach ist festzustellen, dass Art. 83 DSGVO es nicht gestattet, eine Geldbuße wegen eines in Art. 83 Abs. 4 bis 6 genannten Verstoßes zu verhängen, ohne dass nachgewiesen ist, dass dieser Verstoß von dem Verantwortlichen vorsätzlich oder fahrlässig begangen wurde. Folglich ist Voraussetzung für die Verhängung einer solchen Geldbuße, dass der Verstoß schuldhaft begangen wurde.

76 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 (vgl. entsprechend Urteile vom 18. Juni 2013, Schenker & Co. u. a., C-681/11, EU:C:2013:404, Rn. 37 und die dort angeführte Rechtsprechung, vom

25. März 2021, Lundbeck/Kommission, C-591/16 P, EU:C:2021:243, Rn. 156, und vom 25. März 2021, Arrow Group und Arrow Generics/Kommission, C-601/16 P, EU:C:2021:244, Rn. 97).

...

78 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.“

II.3.4. Zum Verhältnis zwischen Unionsrecht und innerstaatlichem Recht:

II.3.4.1. Wenn die Beschwerdeführerin im Rahmen ihres Beschwerdevorbringens, unter Verweis auf § 11 DSG, § 34a VStG und Art. 18 B-VG, zusammengefasst die Rechtsansicht vertritt, dass für die mit dem angefochtenen Straferkenntnis verfolgten – und von der Beschwerdeführerin dem Grunde nach in zwei von drei Spruchpunkten eingeräumten – Verstößen von der belangten Behörde keine Geldbuße zu verhängen, sondern vielmehr mit einer Verwarnung das Auslangen gefunden werden hätte sollen, war dem aus Sicht des erkennenden Senates bereits im Lichte der unmittelbar anwendbaren Vorgaben der Art. 58 und 83 DSGVO – sowie der hierzu einschlägigen Rechtsprechung des EuGH vom 05.12.2023 – nicht zu folgen.

II.3.4.2. Wie vom EuGH in dessen Urteil vom 05.12.2023 zu C-807/21 klar und eindeutig zum Ausdruck gebracht, gilt für die materiellen Voraussetzungen, die eine Aufsichtsbehörde bei der Verhängung einer Geldbuße gegen einen Verantwortlichen zu beachten hat, ausschließlich das Unionsrecht, wobei diese Voraussetzungen in Art. 83 Abs. 1 bis 6 DSGVO genau festgelegt sind (vgl. erneut C-807/21, Rz. 45, 48 und 65). Nach Art. 288 Abs. 2 AEUV ist eine Unionsverordnung in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat, sodass es, sofern nichts anderes bestimmt ist, ausgeschlossen ist, dass die Mitgliedstaaten innerstaatliche Vorschriften erlassen, die die Tragweite einer solchen Verordnung beeinträchtigen. Außerdem dürfen die Mitgliedstaaten aufgrund der ihnen aus dem AEU-Vertrag obliegenden Verpflichtungen die unmittelbare Geltung, die den Verordnungen innewohnt, nicht vereiteln (vgl. erneut EuGH, C-807/21, Rz. 52).

II.3.4.3. Hieraus folgt aber, dass im Anwendungsbereich der DSGVO, kein Raum für die Anwendung der Bestimmungen nach § 11 DSG („Verwarnung durch die Datenschutzbehörde“) und § 33a VStG („Beraten“) verbleibt, da diese Bestimmungen darauf abzielen, der Datenschutzbehörde zusätzliche Vorgaben hinsichtlich deren Ermessensausübung in Bezug auf die von Art. 58 DSGVO eingeräumten Abhilfebefugnisse

aufzugeben. Wenn § 11 DSG unmissverständlich vorgibt, „[i]nsbesondere bei erstmaligen Verstößen wird die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen“, ist diese Bestimmung jedenfalls unvereinbar mit Art. 83 Abs. 2 bis 6 in Verbindung mit Art. 58 Abs. 2 lit. i DSGVO, da diese darauf abzielt, das Ermessen der Datenschutzbehörde, weg von der Verhängung einer Geldbuße im Sinn von Art. 58 Abs. 2 lit. i DSGVO, hin zur Erteilung einer Verwarnung im Sinne von Art. 58 Abs. 2 lit. b DSGVO, zu determinieren.

II.3.4.4. An dieser Stelle ist im Sinne der rezenten Rechtsprechung des EuGH zu Art. 83 DSGVO mit Blick auf das Verwaltungsstrafgesetz (VStG) zu bemerken, dass die Tatsache, wonach die DSGVO den Mitgliedstaaten die Möglichkeit einräumt, Anforderungen an das von den Aufsichtsbehörden anzuwendende Verfahren bei der Verhängung einer Geldbuße vorzusehen, keineswegs bedeutet, dass sie auch befugt wären, über diese verfahrensrechtlichen Anforderungen hinaus materielle Voraussetzungen vorzusehen, die zu den in Art. 83 Abs. 1 bis 6 DSGVO geregelten hinzutreten. Des Weiteren wird durch den Umstand, dass der Unionsgesetzgeber eigens und ausdrücklich diese Möglichkeit vorgesehen hat, aber nicht diejenige, solche zusätzlichen materiellen Voraussetzungen festzulegen, bestätigt, dass er den Mitgliedstaaten insoweit keinen Ermessensspielraum gelassen hat. Für diese materiellen Voraussetzungen gilt daher ausschließlich das Unionsrecht (vgl. erneut EuGH vom 05.12.2023, C-807, Rz. 46, 48). Vor diesem Hintergrund verbleibt auch für die Bestimmungen in § 5 VStG („Schuld“), das Verschulden des Verantwortlichen ist ausschließlich anhand der Bestimmungen des Art. 83 Abs. 1 und Abs. 2 DSGVO zu beurteilen, § 7 VStG („Anstiftung und Beihilfe“), eine Form der Beitragstäterschaft ist von Art. 83 DSGVO nicht vorgesehen und mit der Regelungssystematik von Art. 83 DSGVO nicht in Einklang zu bringen, § 9 VStG („Besondere Fälle der Verantwortlichkeit“), die Strafbarkeit juristischer Personen und eingetragener Personengesellschaften richtet sich ausschließlich nach der Systematik des Art. 4 Z 7 iVm Art. 83 DSGVO und kann deren Haftung nicht auf zur Vertretung nach außen Berufene oder auf einen verantwortlichen Beauftragten überwältzt werden, § 19 VStG („Strafbemessung“), die Bemessung der Geldbuße erfolgt ausschließlich anhand der von Art. 83 Abs. 1 bis 6 DSGVO normierten Kriterien, § 20 VStG („Außerordentliche Milderung der Strafe“), die Erschweris- und Milderungsgründe ergeben sich abschließend aus Art. 83 Abs. 2 DSGVO, § 22 Abs. 2 VStG („Zusammentreffen von strafbaren Handlungen“), Art. 83 Abs. 3 DSGVO regelt das Zusammentreffen mehrerer Verstöße abschließend, im Anwendungsbereich der DSGVO kein Raum und haben daher unangewendet zu bleiben (vgl. EuGH vom 05.12.2023, C-683/21, Rz 70).

II.3.5. Zur Anfechtung von Spruchpunkt III dem Grunde nach:

II.3.5.1. Die Beschwerdeführerin richtet sich mit ihrer Beschwerde in Bezug auf Spruchpunkt III. des angefochtenen Bescheides nicht nur gegen die Strafhöhe, sondern auch gegen die rechtliche Feststellung des Verstoßes gegen die Verpflichtungen aus Art. 33 DSGVO dem Grunde nach. Hierzu im Einzelnen:

II.3.5.2. Mit Spruchpunkt III. des hier angefochtenen Straferkenntnisses hat die belangte Behörde ausgesprochen, die Beschwerdeführerin habe in ihrer Rolle als Verantwortliche im Zeitraum vom 05.04.2023 bis 22.06.2023 innerhalb des Bundesgebietes Österreich gegen ihre Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Datenschutzbehörde gemäß Art. 33 Abs. 1 DSGVO verstoßen, indem sie die unter Spruchpunkt I. dargestellte Verletzung des Schutzes der personenbezogenen Daten der Betroffenen durch die unbefugte Offenlegung deren (Gesundheits-)Daten gegenüber Dritten nicht unverzüglich und möglichst binnen 72 Stunden, nachdem diese Verletzung der Beschwerdeführerin bekannt wurde, der Datenschutzbehörde gemeldet habe.

II.3.5.3. Zwar räumt die Beschwerdeführerin – zuletzt auch in der mündlichen Verhandlung vor dem Bundesverwaltungsgericht – ein, zu keinem Zeitpunkt eine Meldung nach Art. 33 DSGVO an die Datenschutzbehörde betreffend die gegenständliche Offenlegung im Zuge der Terminerinnerung vom 05.04.2023 erstattet zu haben, eigenen Aussagen zufolge waren ihr allfällige diesbezügliche Pflichten aus der DSGVO auch gar nicht bekannt. Die Beschwerdeführerin vertritt diesbezüglich einerseits die Rechtsansicht, dass eine derartige Meldung – auch nach Inanspruchnahme rechtsanwaltlicher Beratung – als nicht (mehr) erforderlich und zweckmäßig erachtet worden sei, da die belangte Behörde vom Vorfall ohnehin bereits – wenn auch von dritter Seite – in Kenntnis gesetzt worden sei und die Beschwerdeführerin mit Schreiben vom 05.06.2023 zur Stellungnahme im Rahmen eines behördlichen Prüfverfahrens aufgefordert hatte; andererseits bestehe aus Sicht der Beschwerdeführerin die Verpflichtung zur Meldung nach Art. 33 Abs. 1 DSGVO – in Zusammenschau mit dem 85. Erwägungsgrund – *„nur in Fällen, in welchen – aus dem Blickwinkel der Verantwortlichen betrachtet, also soweit für diese voraussichtlich erkennbar und abschätzbar“*, die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt; es sei zusammengefasst fraglich, ob durch die fallgegenständliche, versehentliche, einmalige Offenlegung von Telefonnummern im Zuge der Terminerinnerungsnachricht ein im Sinne der Vorgaben des Art. 33 DSGVO relevantes Risiko ausgegangen sei.

Dem diesbezüglichen Rechtsstandpunkt der Beschwerdeführerin war aus den nachfolgenden Gründen nicht zu folgen:

II.3.5.4. Wie festgestellt, hat die Ordinationsassistentin der Beschwerdeführerin am 05.04.2023 die inkriminierte Text-Nachricht zur Erinnerung an Termine für den 06.04.2023, dies in Form einer Gruppentextnachricht an insgesamt 27 Personen als Empfänger versandt, wobei es sich bei den Empfängern um Patienten der Ordination der Beschwerdeführerin handelte. Die Telefonnummern der einzelnen Empfänger stellen jedenfalls personenbezogene Daten der Empfänger im Sinne von Art. 4 Z 1 DSGVO dar, ebenso der aus dem Kontext der Nachricht hervorgehende Umstand, dass die Empfänger das Dienstleistungsangebot der Beschwerdeführerin als Fachärztin für Psychiatrie bzw. als Psychotherapeutin in Anspruch nehmen. Letztere Informationen sind zudem als „Gesundheitsdaten“ im Sinne von Art. 4 Z 15 DSGVO zu qualifizieren, da aus dem Gesamtkontext der Nachricht zumindest indirekt ableitbar ist, dass sich die Empfänger aufgrund einer psychischen Erkrankung in Behandlung befinden (vgl. EuGH vom 01.08.2022, C-184/20, Rz 125 ff). Die gesamte Vorgangsreihe von der Erstellung der Gruppen-Textnachricht auf dem Mobiltelefon der Ordination bis zum Versand der Nachricht stellt eine Verarbeitung im Sinne von Art. 4 Z 2 DSGVO in Form der Verwendung und Offenlegung durch Übermittlung dar. Wie festgestellt, hat die Beschwerdeführerin als Inhaberin der Ordination ihre Ordinationsassistentin angewiesen, die Textnachrichten zur Terminerinnerung mit dem Praxis-Telefon zu versenden, wodurch die Beschwerdeführerin als Verantwortliche im Sinne von Art. 4 Z 7 DSGVO für den gesamten Vorgang anzusehen ist, da sie aus Eigeninteresse auf die Verarbeitung der in Rede stehenden (Gesundheits-)Daten Einfluss genommen hat und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitgewirkt hat. Hierbei ist es nicht erforderlich, dass über die Zwecke und Mittel der Verarbeitung mittels schriftlicher Anleitungen oder Anweisungen seitens der Verantwortlichen – hier: seitens der Beschwerdeführerin gegenüber deren Ordinationsgehilfen – entschieden wurde (vgl. EuGH vom 05.12.2023, C-683/21, Rz 30 ff).

II.3.5.5. Die in der DSGVO vorgesehenen Grundsätze, Verbote und Pflichten richten sich insbesondere an „Verantwortliche“. Deren Verantwortung und Haftung erstreckt sich nach den Ausführungen im 74. Erwägungsgrund der DSGVO auf jedwede Verarbeitung personenbezogener Daten, die durch sie oder in ihrem Namen erfolgt. In diesem Rahmen müssen sie nicht nur geeignete und wirksame Maßnahmen treffen, sondern sie müssen auch nachweisen können, dass ihre Verarbeitungstätigkeiten im Einklang mit der DSGVO stehen und die Maßnahmen, die sie ergriffen haben, um diesen Einklang sicherzustellen, auch wirksam sind. Diese Haftung ist es, die bei einem der in Art. 83 Abs. 4 bis 6 DSGVO genannten

Verstöße die Grundlage dafür bildet, nach Art. 83 DSGVO eine Geldbuße gegen den Verantwortlichen zu verhängen (vgl. erneut EuGH vom 05.12.2023, C-807/21, Rz 38).

II.3.5.6. Bereits aus dem klaren und eindeutigen Wortlaut des Art. 33 Abs. 1 DSGVO ergibt sich die Verpflichtung des Verantwortlichen, im Falle der Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der Datenschutzbehörde unter Einhaltung der inhaltlichen Vorgaben des Art. 33 Abs. 3 DSGVO zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dieser objektiven Verpflichtung ist die Beschwerdeführerin als für sämtliche Datenverarbeitungsvorgänge, die im Zusammenhang mit deren Tätigkeit als niedergelassene Fachärztin stehen, Verantwortliche im Sinne von Art. 4 Z 7 DSGVO nicht nachgekommen. Dies bereits deshalb nicht, da sie von den Vorgaben der DSGVO im Allgemeinen, und der Pflicht zur Meldung von Sicherheitsvorfällen gemäß Art. 33 DSGVO, im Besonderen, keinerlei Kenntnis hatte.

II.3.5.7. Wenn die Beschwerdeführerin rechtlich in Frage stellt, ob im gegebenen Zusammenhang die versehentliche Offenlegung der in der Gruppen-Textnachricht enthaltenen Informationen – wie von Art. 33 Abs. 1 erster Satz DSGVO gefordert – „voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen“ geführt hat und daher fraglich sei, ob eine Pflicht zur Meldung des Vorfalles vom 05.04.2023 fallbezogen überhaupt bestanden habe, so kann aus diesem Einwand für den Rechtsstandpunkt der Beschwerdeführerin nichts gewonnen werden. Vielmehr stellt die – wenn auch unbeabsichtigte – Offenlegung der Informationen aus der Gruppen-Textnachricht bei verständiger Betrachtung ein (erhebliches) Risiko für die Rechte und Freiheiten der betroffenen Personen dar. Die gegenständliche Offenlegung des – zumindest mittelbar – aus den Gesamtkontext der Gruppen-Textnachricht hervorgehenden Umstandes, wonach die jeweiligen Empfänger der Nachricht sich aufgrund einer psychischen Erkrankung in Behandlung befinden oder zumindest die Dienstleistungen einer Psychotherapeutin in Anspruch nehmen, kann aus Sicht des erkennenden Senates jedenfalls zu einem physischen, materiellen oder immateriellen Schaden auf Seiten der Betroffenen führen. In Betracht kommt fallbezogen das Risiko einer Diskriminierung, finanzielle Verluste etwa durch Verlust eines Arbeitsplatzes in einem sensiblen Bereich der eine hohe körperliche und geistige Leistungsfähigkeit voraussetzt, eine Rufschädigung sowie der Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten sowie andere gesellschaftliche Nachteile für die betroffene natürliche Person (vgl. hierzu auch den 85. Erwägungsgrund zur DSGVO).

II.3.5.8. Der Umstand, dass die Beschwerdeführerin im gegenständlichen Fall ihre Pflicht im Sinne von Art. 33 Abs. 1 DSGVO zur Meldung des Sicherheitsvorfalles an die Datenschutzbehörde gar nicht kannte, und/oder – bezogen auf den speziellen Anlassfall – nicht erkannte, führt dabei nicht zur Entlastung der Beschwerdeführerin. Vielmehr wäre es die Pflicht der Beschwerdeführerin in deren Eigenschaft als datenschutzrechtlich Verantwortliche gewesen, sich mit den einschlägigen, aus der DSGVO resultierenden Verpflichtungen vertraut zu machen, ihre Mitarbeiter der Ordination in ausreichendem Ausmaß zu schulen und anzuleiten und für die Einhaltung der datenschutzrechtlichen Vorgaben im Zusammenhang mit dem Betrieb ihrer Ordination auf wirksame Weise Sorge zu tragen; es kann – entgegen dem Vorbringen der Beschwerdeführerin – auch keinesfalls als Aufgabe der Aufsichtsbehörde angesehen werden, Verantwortliche auf die Pflicht zur Meldung eines erfolgten Sicherheitsvorfalles aufmerksam zu machen oder eine solche zu erwirken, vielmehr ist es allein die Aufgabe eines Verantwortlichen, die sich aus der DSGVO ergebenden Pflichten einzuhalten (vgl. erneut EuGH vom 05.12.2023, C-807/21, Rz 38, sowie C-883/21, Rz 80, 81). Auch in den vom Europäischen Datenschutzausschuss veröffentlichten Leitlinien betreffend der Meldung von Sicherheitsverletzungen nach Art. 33 DSGVO werden die verbindlichen Melde- und Benachrichtigungsanforderungen der DSGVO erläutert und Maßnahmen vorgestellt, die die Verantwortlichen und Auftragsverarbeiter zur Erfüllung dieser Verpflichtungen ergreifen können. Außerdem werden Beispiele für verschiedene Arten von Datenschutzverletzungen beschrieben, um anhand unterschiedlicher Szenarien zu erläutern, wer jeweils unterrichtet werden muss (vgl. EDSA- Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, angenommen am 03.10.2017, zuletzt überarbeitet am 28.03.2023).

II.3.5.9. Im Ergebnis war daher festzustellen, dass die Beschwerdeführerin, als datenschutzrechtlich Verantwortliche im Sinne von Art. 4 Z 7 DSGVO, indem sie im Nachgang zur verfahrensgegenständlichen Sicherheitsverletzung, der Offenlegung von Gesundheitsdaten durch Übermittlung einer Terminerinnerungsnachricht an 27 Empfänger am 05.04.2023, keine Benachrichtigung an die Datenschutzbehörde vorgenommen hat, gegen ihre Pflichten nach Art. 33 DSGVO verstoßen hat. Im vorliegenden Zusammenhang liegt jedenfalls Verschulden in Form von Fahrlässigkeit vor, da die Beschwerdeführerin als Betreiberin einer fachärztlichen Praxis verpflichtet gewesen wäre, sich Kenntnis über die einschlägigen datenschutzrechtlichen Vorgaben zu verschaffen und deren Einhaltung im Rahmen ihres Ordinationsbetriebes effektiv sicherzustellen. Die Unterlassung all dessen ist als objektiv sorgfaltswidrig anzusehen. Der diesbezüglich ergangene Ausspruch in Spruchpunkt III. des angefochtenen Bescheides ist daher zu Recht ergangen.

II.3.6. Zur Strafzumessung:

II.3.6.1. Zunächst ist festzuhalten, dass – wie bereits unter II.3.4.2. dargestellt – für die materiellen Voraussetzungen, die eine Aufsichtsbehörde bei der Verhängung einer Geldbuße gegen einen Verantwortlichen zu beachten hat, ausschließlich das Unionsrecht maßgebend ist, wobei diese Voraussetzungen in Art. 83 Abs. 1 bis 6 DSGVO genau festgelegt sind (vgl. erneut EuGH, Urteile vom 05.12.2023, C-807/21, Rz 45, 48, 52 und 65 sowie C-683/21, Rz 64 bis 70).

II.3.6.2. Wie bereits unter II.3.4.4. dargelegt, verbleibt im Anwendungsbereich der DSGVO auch in Bezug auf die vorzunehmende Strafzumessung kein Raum für die Anwendung nationaler Bestimmungen, hier etwa der § 5, 19, 20 und 22 des Verwaltungsstrafgesetzes - VStG. Eine Bedachtnahme auf die Bestimmung des § 19 VStG und die hierzu ergangene Rechtsprechung, hat – entgegen den Ausführungen unter Punkt 4.2. des angefochtenen Bescheides – nicht Platz zu greifen. Fallbezogen war die Strafzumessung jedoch ohnehin vom Bundesverwaltungsgericht – aufgrund und im Lichte des Beschwerdevorbringens – zu überprüfen.

Was die Anwendung der Bestimmung des § 16 VStG zur Festsetzung einer Ersatzfreiheitsstrafe für den Fall der Uneinbringlichkeit der verhängten Geldbuße betrifft, so bestehen gegen diese Bestimmung im Lichte des Art. 84 Abs. 1 DSGVO keine unionsrechtlichen Bedenken.

II.3.6.3. Zur (Nicht-)Erteilung einer Verwarnung anstelle der Verhängung einer Geldbuße:

II.3.6.3.1. Die Beschwerdeführerin begehrt im Rahmen ihres Rechtsmittelvorbringens sowie ihren Erklärungen im Rahmen der mündlichen Verhandlung primär, anstelle der Verhängung einer Geldbuße im vorliegenden Fall mit der Erteilung einer Verwarnung das Auslangen zu finden, da die gegenständliche Offenlegung lediglich einmalig und versehentlich erfolgte. Dem diesbezüglichen Begehren kann aufgrund der nachstehenden Erwägungen nicht entsprochen werden:

II.3.6.3.2. Zwar bestimmt Art. 58 Abs. 2 lit. i DSGVO, dass die Aufsichtsbehörden befugt sind, eine Geldbuße gemäß Art. 83 DSGVO „zusätzlich zu oder anstelle von“ anderen in Art. 58 Abs. 2 genannten Abhilfebefugnissen wie die Befugnis zur Erteilung von Warnungen, Verwarnungen oder Anweisungen zu verhängen. Ebenso heißt es im 148. Erwägungsgrund dieser Verordnung u. a., dass es den Aufsichtsbehörden gestattet ist, im Fall eines geringfügigeren Verstoßes oder falls die voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, von der Verhängung einer Geldbuße abzusehen und stattdessen eine Verwarnung zu erteilen.

II.3.6.3.3. Im vorliegenden Fall kann der mit Spruchpunkt I des angefochtenen Bescheides geahndete Verstoß, also die (unbeabsichtigte) Offenlegung der Gesundheitsdaten an 27 Empfänger im Rahmen einer Terminerinnerungsnachricht und die damit einhergehende Verletzung der Vertraulichkeit von gesundheitsbezogenen Informationen, keinesfalls als geringfügiger Verstoß, der das Absehen von einer Geldbuße ermöglichen würde, qualifiziert werden. Dies bereits deshalb nicht, da es sich bei den betroffenen personenbezogenen Daten um Gesundheitsdaten handelt, deren Verarbeitung auf Seiten des Verantwortlichen jedenfalls ein besonderes Maß an Sorgfalt erfordert. Gerade dieses Maß an Sorgfalt hat die Beschwerdeführerin in ihrer Eigenschaft als Verantwortliche jedoch gänzlich vermissen lassen.

II.3.6.3.4. So hat sie sich weder mit den datenschutzrechtlichen Rahmenbedingungen im Zusammenhang mit ihrer Tätigkeit als niedergelassene Fachärztin vertraut gemacht, obwohl der Betrieb einer Arztpraxis regelmäßig mit der Verarbeitung von Gesundheitsdaten im Sinne von Art. 4 Z 15 DSGVO – nicht bloß geringfügigen Ausmaßes – einhergeht, und damit naturgemäß ein erhöhtes Risiko für die Rechte betroffener Personen besteht. Die Verantwortliche hat – in Ermangelung jedweder datenschutzrechtlicher Kenntnis – auch keine dem Risiko angemessenen technischen und organisatorischen Maßnahmen zum Schutz der Vertraulichkeit der verarbeiteten personenbezogenen Daten ergriffen. Andernfalls hätte sie zur Umsetzung eines Benachrichtigungssystems zur Terminerinnerung für Patienten eine geeignete technische Lösung zum Einsatz gebracht, die dem Stand der Technik entspricht und vielfältig am Markt angeboten und verwendet wird. Der Versand von Gruppennachrichten, sei es per SMS- E-Mail oder Messenger-Diensten, ist für den hier verfolgten Zweck jedenfalls völlig ungeeignet, da das Zusammenfassen mehrerer Empfänger zu einer Gruppe darauf abzielt, bestimmte Inhalte sämtlichen Empfängern zugänglich zu machen. Gegenteilige Anforderungen sind jedoch an ein Benachrichtigungssystem zur Terminerinnerung an Patienten einer Arztpraxis zu stellen, die fraglichen Informationen sollen ausschließlich den betreffenden Patienten persönlich erreichen, nicht aber auch andere Personen.

II.3.6.4. Zum Beschwerdevorbringen, wonach die mit dem angefochtenen Straferkenntnis verhängte Geldbuße unangemessen hoch erscheine:

II.3.6.4.1. Die Beschwerdeführerin bringt im Rahmen ihrer Beschwerde weiterhin vor, ihr sei trotz mehrfacher Verfehlungen [gegen die DSGVO] insgesamt nur ein geringes Verschulden anzulasten, da die inkriminierte Offenlegung durch Übermittlung „*Terminerinnerung mittels SMS*“ vor deren Verwendung zunächst getestet worden sei, die „(zuvor unbekannte) Funktionsweise des Betriebssystems, konkret der Versand von Terminerinnerungen als „iMessage“ und nicht als „SMS“, wenn sich unter den Empfängern auch iPhone-Nutzer befinden, im Zuge des Testbetriebs jedoch niemals in Erscheinung getreten sei. Im Übrigen verweist die

Beschwerdeführerin darauf, dass sie über jene Verpflichtungen, deren Missachtung ihr nunmehr angelastet wurden, keine ausreichenden Informationen gehabt habe und ihr nicht bewusst gewesen sei, welche Pflichten sich aus den datenschutzrechtlichen Vorgaben für sie tatsächlich ergeben hätten.

II.3.6.4.2. Mit ihrem diesbezüglichen Vorbringen zielt die Beschwerdeführerin auf eine (erhebliche) Reduktion der verhängten Geldbuße ab.

II.3.6.4.3. Nach Art. 83 Abs. 1 DSGVO stellt jede Aufsichtsbehörde sicher, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. In Art. 83 Abs. 2 DSGVO sind Zumessungskriterien aufgeführt, die bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag in jedem Einzelfall "gebührend" zu berücksichtigen sind. Relevant sind danach insbesondere Art, Schwere und Dauer des Verstoßes, die Zahl der von der Verarbeitung betroffenen Personen, das Ausmaß des Schadens, die Kategorie der betroffenen personenbezogenen Daten, das Bemühen des Unternehmens, den Schaden zu begrenzen, Art und Umfang der Kooperation mit den Datenschutzbehörden und der Grad der Verantwortlichkeit.

II.3.6.4.4. Mit dem angefochtenen Straferkenntnis verhängte die Datenschutzbehörde eine (einheitliche) Geldbuße im Sinne von Art. 83 Abs. 3 DSGVO aufgrund der Verwirklichung mehrerer Verstöße gegen Bestimmungen der DSGVO in Form „gleicher oder miteinander verbundener Verarbeitungsvorgänge“ (Tateinheit - Idealkonkurrenz). Spruchpunkt I. bezieht sich dabei auf den Vorwurf der (fahrlässigen) unrechtmäßigen Offenlegung von Gesundheitsdaten durch Übermittlung in Form einer Gruppen-Textnachricht am 05.04.2023, Spruchpunkt II. betrifft den Vorwurf, die Verantwortliche habe im Zeitraum von XXXX bis 22.06.2023 gegen die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 1 DSGVO verstoßen, indem sie kein Verzeichnis aller Verarbeitungstätigkeiten, die im Tatzeitraum ihrer Zuständigkeit unterlagen, in der nach Art. 30 Abs. 3 DSGVO genannten Form geführt und folglich entgegen Art. 30 Abs. 4 DSGVO der Behörde auch nicht zur Verfügung gestellt habe; Spruchpunkt III. betrifft schließlich den Vorwurf, die Verantwortliche habe vom 05.04.2023 bis 22.06.2023 gegen ihre Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Datenschutzbehörde gemäß Art. 33 Abs. 1 DSGVO verstoßen, indem Sie die unter Punkt I. dargestellte Verletzung des Schutzes der personenbezogenen Daten durch die unbefugte Offenlegung von (Gesundheits-)Daten gegenüber Dritten nicht unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung der Beschwerdeführerin in deren Rolle als Verantwortliche bekannt wurde, der Datenschutzbehörde gemeldet habe.

II.3.6.4.5. Art. 83 Abs. 3 DSGVO legt fest, dass in Fällen wie im vorliegenden, in denen ein Verantwortlicher bei „gleichen oder miteinander verbundenen Verarbeitungsvorgängen“ vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung verstößt, der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß übersteigt.

II.3.6.4.6. Der Begriff „miteinander verbunden“ bezieht sich dabei auf den Grundsatz, dass ein einheitliches Verhalten aus mehreren Teilen bestehen kann, deren Ausführung von einem einheitlichen Willen bestimmt ist und die inhaltlich (insbesondere in Bezug auf die Identität der betroffenen Person, den Zweck und die Art), räumlich und zeitlich so eng miteinander verbunden sind, dass sie objektiv als eine natürliche Handlungseinheit angesehen werden können (vgl. EDSA Leitlinien 2023 zu Art. 83 DSGVO, Rz 28). Dies ist im vorliegenden der Fall, da die unrechtmäßige Offenlegung in engem Zusammenhang mit dem sonstigen Verhalten der Verantwortlichen, näherhin der gänzlichen Unkenntnis datenschutzrechtlicher Verpflichtungen im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen des Betriebes der Arztpraxis, steht, dass auch zur Verwirklichung der Verletzung der Pflichten nach Art. 30 und 33 DSGVO im Sinne einer natürlichen Handlungseinheit führte.

II.3.6.4.7. Die DSGVO normiert damit für bestimmte Fallkonstellationen ein Absorptionsprinzip, dies in Abweichung zu dem ansonsten von § 22 Abs. 2 VStG normierten Kumulationsprinzip.

Im vorliegenden Fall besteht der „schwerwiegendste Verstoß“ in der mit Spruchpunkt I. des angefochtenen Bescheides verfolgten unrechtmäßigen Offenlegung von Gesundheitsdaten, wodurch die Verantwortliche die Bestimmungen der Art. 5 Abs. 1 und Art. 9 DSGVO verletzt hat. Für Verstöße gegen die vorgenannten Bestimmungen gilt der Strafrahmen des Art. 83 Art. 5 lit. a DSGVO, sohin ein Rahmen bis 20.000.000 EURO, auch wenn die Verantwortliche im vorliegenden Zusammenhang Unternehmerin ist, kommt der umsatzbezogene Strafrahmen von bis zu 4 Prozent des weltweit erzielten Jahresumsatzes mit Blick auf das – wenn auch nur geschätzte Einkommen der Verantwortlichen – nicht in Betracht.

Auch in Fällen des Art. 83 Abs. 3 DSGVO ist jedoch – auch nach Ansicht des Europäischen Datenschutzausschusses – zu beachten, dass der Wortlaut „Gesamtbetrag“ in Art. 83 Abs. 3 DSGVO indiziert, dass alle begangenen Verstöße bei der Beurteilung des Betrags der Geldbuße berücksichtigt werden müssen und die Formulierung „Betrag für den schwerwiegendsten Verstoß“ sich auf das gesetzliche Höchstmaß für Geldbußen bezieht (Art. 83 Abs. 4 bis 6 DSGVO). Daher ist, auch wenn die Geldbuße nicht die rechtliche Höchstgrenze der höchsten Bußgeldstufe übersteigen darf, ein Verantwortlicher für schuldig zu befinden, gegen mehrere Bestimmungen verstoßen zu haben. Diese Verstöße müssen bei der Beurteilung des Betrags der endgültigen Geldbuße, die zu verhängen ist, entsprechend Berücksichtigung finden. In

Fällen, wie dem vorliegenden, in dem die Verantwortliche durch Tateinheit mehrere Verstöße gegen die DSGVO verwirklicht, hier neben Art. 5 und 9 DSGVO auch die Pflichten aus Art. 30 und 33 DSGVO, können die übrigen – neben dem als schwerwiegendsten Verstoß identifizierten – begangenen Verstöße nicht verworfen werden, sondern müssen bei der Berechnung der Geldbuße berücksichtigt werden (vgl. EDSA Leitlinien 2023 zu Art. 83 DSGVO, Rz. 43).

II.3.6.4.8. Zu den Erschwerungsgründen ist fallbezogen festzuhalten:

II.3.6.4.8.1. Der belangten Behörde ist zunächst vollinhaltlich zuzustimmen, wenn diese unter Punkt 4.12. des angefochtenen Bescheides zusammengefasst feststellt, dass durch die gegenständliche Verarbeitung sensible Daten in Form von Gesundheitsdaten der betroffenen Personen gegenüber unbefugten Personen offengelegt wurden und die gegenständlichen Informationen neben den Datenschutzgrundsätzen nach Art. 5 Abs. 1 DSGVO auch einer gesetzlichen Verschwiegenheitsverpflichtung unterliegen, die die Beschuldigte in ihrer Rolle als Fachärztin zu gewährleisten hat, sowie dass die Beschuldigte durch die von ihr zu verantwortenden Verstöße gegenüber unbefugten Dritte de facto eine Liste ihrer Patienten mit einem Termin in ihrer Ordination offengelegt hat, wobei die Information, dass sich eine bestimmte Person in psychotherapeutischer Behandlung befindet und in diesem Zusammenhang bereits einen Termin bei einer bestimmten Fachärztin mit konkreten Schwerpunkten vereinbart hat, einem besonderen Geheimhaltungsinteresse der betroffenen Personen unterliegen. Nicht zu beanstanden ist daher die Einordnung der belangten Behörde, wonach der durch die gegenständlichen Verstöße erfolgte Eingriff in das Grundrecht der betroffenen Personen auf Geheimhaltung ihrer personenbezogenen Daten (§ 1 Abs. 1 DSG; Art. 7 und 8 EU-GRC; Art. 8 EMRK) einen gravierenden Eingriff darstellt und diese Faktoren im Zuge der Strafbemessung besonders ins Gewicht zu fallen haben (Art. 83 Abs. 2 lit. a DSGVO). Zu berücksichtigen ist jedoch nach Ansicht des erkennenden Senates hierbei, dass eine Verknüpfung der vorliegend offengelegten Telefonnummern mit einer namentlich identifizierbaren Person zumindest mit einem gewissen Aufwand verbunden ist, sodass sich hieraus ein geringfügige Minderung der Einschätzung in Bezug auf die Schwere des Eingriffs und eine damit verbundene Reduktion der Geldbuße ergibt.

II.3.6.4.8.2. Wenn die Behörde jedoch – unter Heranziehung von Art. 83 Abs. 2 lit. g DSGVO – als weiteren Erschwerungsgrund den Umstand verwertet, dass durch den zu ahndenden Verstoß besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO betroffen waren, liegt nach Ansicht des erkennenden Senates hierin eine doppelte (und damit unzulässige) Verwertung ein und desselben Erschwerungsgrundes vor. So fand der rechtliche Umstand, dass im Zuge des Verstoßes besonders geschützte Informationen der Betroffenen

zur Inanspruchnahme von Gesundheitsdienstleistungen einer Facharztpraxis für Psychiatrie und Psychologie offengelegt wurden, bereits Eingang in die Bewertung des Verstoßes hinsichtlich der Art, der Schwere und des Umfanges des Verstoßes im Sinne von Art. 83 Abs. 2 lit. a DSGVO. Im Besonderen aus diesem Grund hatte die im Spruch vorgenommene Reduktion der verhängten Geldbuße zu erfolgen.

II.3.6.4.8.3. Eine weitere Reduktion der verhängten Geldbuße war aus den nachstehenden Gründen nicht geboten:

Wie bereits oben unter Punkt 3.5. ausgeführt, hat die Beschwerdeführerin in deren Rolle als Verantwortliche im Zusammenhang mit ihrer Facharztpraxis keinerlei Schritte unternommen, um sich mit den geltenden datenschutzrechtlichen Bestimmungen im Zusammenhang mit der Verarbeitung personenbezogener (Gesundheits-)Daten vertraut zu machen und die Einhaltung der DSGVO im Zuge ihrer unternehmerischen Tätigkeit sicherzustellen. Nach Ansicht des erkennenden Senates muss aber von datenschutzrechtlich Verantwortlichen, wenn diese selbständig als Facharzt bzw. Fachärztin unternehmerisch tätig sind, erwartet werden können, sich mit den grundlegenden Vorgaben der DSGVO vertraut zu machen, dies insbesondere mit Blick auf die Rahmenbedingungen im Zusammenhang mit der im ärztlichen Bereich regelmäßig vorzunehmenden Verarbeitung von Gesundheitsdaten, im Besonderen mit den Erlaubnistatbeständen des Art. 9 Abs. 2 DSGVO, den Rechten der Betroffenen gemäß Art. 15 ff DSGVO, sowie der erforderlichen technischen und organisatorischen Maßnahmen im Sinne von Art. 5 Abs. 1 lit. f IVm Art. 32 DSGVO zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus bei der Verarbeitung von Gesundheitsdaten. Werden in einer Ordination Terminerinnerungen mittels SMS ausgesandt, muss dafür vorab zunächst eine ausdrückliche Einwilligung des Patienten gemäß Art. 9 Abs. 2 lit. a DSGVO eingeholt werden, da eine SMS-Erinnerung mangels Erforderlichkeit für die ärztliche Berufsausübung nicht auf den Ausnahmetatbestand des Art 9 Abs. 2 lit. h DSGVO gestützt werden kann.

Demgegenüber kannte die Beschwerdeführerin in deren Rolle als Verantwortliche nicht die Vorgaben des Art. 9 Abs. 1 und Abs. 2 DSGVO, hat daher keine ausdrückliche Einwilligungserklärung für die Terminerinnerungsbenachrichtigung per SMS eingeholt, kannte zudem die Verpflichtung zur Führung eines Verarbeitungsverzeichnisses im Sinne von Art. 30 Abs. 1 und Abs. 5 DSGVO nicht, waren ihr die Pflichten aus Art. 33 DSGVO zur Meldung von Sicherheitsvorfällen unbekannt und setzte sie zur Umsetzung der Terminerinnerungsfunktion an Patienten eine technisch gänzlich ungeeignete – da nicht sichere – Lösung ein.

Die vorgenannten Handlungen und Unterlassungen waren als grob fahrlässiges Verhalten auf Seiten der Beschwerdeführerin in deren Rolle als Verantwortliche zu qualifizieren (Art. 83 Abs. 2 lit. b und lit. d DSGVO). Hervorzuheben ist in diesem Zusammenhang erneut, dass von

niedergelassenen Ärzten im Umgang mit Patientendaten ein besonders hohes Maß an Sorgfalt zur Gewährleistung der gebotenen Sicherheit und Vertraulichkeit zu erwarten ist, die Beschwerdeführerin dieses Maß an Sorgfalt jedoch durch ihre datenschutzrechtliche Unkenntnis und durch die Wahl ungeeigneter technischer Mittel zur Patientenkommunikation gänzlich vermissen hat lassen (vgl. erneut EuGH vom 05.12.2023, C-683/21, Rz. 81, wonach gegen Verantwortliche Sanktionen verhängt werden können, wenn sich der Verantwortliche über die Rechtswidrigkeit seines Verhaltens nicht im Unklaren sein konnte, gleichviel, ob ihm dabei bewusst war, dass es gegen die Bestimmungen der DSGVO verstößt).

Zudem war bei der Strafzumessung erschwerend im Sinne von Art. 83 Abs. 2 lit. k DSGVO zu berücksichtigen, dass die Verantwortliche mit der im vorliegenden Fall als Tateinheit zu qualifizierenden Tathandlung mehrfache Verstöße gegen Bestimmungen der DSGVO verwirklicht hat, konkret neben Art. 5 Abs. 1 in Verbindung mit Art. 9 Abs. 1 und Abs. 2 DSGVO auch die Vorgaben der Art. 30 und 33 DSGVO.

II.3.6.4.9. Mildernd berücksichtigte die belangte Behörde die fahrlässige Begehung, das Nichtvorliegen früherer Verstöße bei der belangten Behörde gegen die DSGVO, die Mitwirkung der Beschwerdeführerin im gegenständlichen Ermittlungsverfahren vor der Datenschutzbehörde, die Anpassung der technischen Einstellungen zur Terminerinnerung von Patienten im Laufe des Verfahrens sowie die nachträgliche Erstellung eines Verarbeitungsverzeichnisses. Weitere Milderungsgründe sind bis zum Zeitpunkt der Entscheidung des erkennenden Gerichtes nicht hervorgekommen.

II.3.6.4.10. Ergebnis: Die vom Bundesverwaltungsgericht errechnete Geldbuße scheint tat- und schuldangemessen und befindet sich am unteren Ende des zur Verfügung stehenden Strafrahmens. Für eine weitere Herabsetzung der Sanktion besteht insbesondere aufgrund der oben genannten Erschwerungsgründe kein Raum. Ein (noch) niedrigerer Betrag würde im vorliegenden Fall den in Art. 83 Abs. 1 DSGVO normierten Kriterien für eine Geldbuße, wonach diese in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein muss, nicht mehr gerecht werden.

II.3.6.4.11. **Zu den Kosten des Verwaltungsstrafverfahrens sowie des Beschwerdeverfahrens**

Gemäß § 64 Abs. 1 VStG ist im Straferkenntnis auszusprechen, dass der Bestrafte einen Beitrag zu den Kosten des Strafverfahrens zu leisten hat. Gemäß § 64 Abs. 2 VStG ist dieser Beitrag für das Verfahren erster Instanz mit 10 % der verhängten Strafe, mindestens jedoch mit 10 Euro zu bemessen. Der Beitrag zu den Kosten war aufgrund der nunmehr verhängten Strafe auf 450,00 Euro zu reduzieren.

Da damit der Beschwerde teilweise Folge gegeben wurde, waren der Beschwerdeführerin keine Kosten des Beschwerdeverfahrens aufzuerlegen (§ 52 Abs. 1 und Abs. 2 VwGVG).

II.3.7. Zu Spruchpunkt B) – Unzulässigkeit 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 gegenständliche Rechtsprechung steht im Einklang mit der Rechtsprechung der Höchstgerichte. Aufgrund der eindeutigen Rechtslage handelt es sich nicht um eine Rechtsfrage grundsätzlicher Bedeutung. Auch liegen keine sonstigen Hinweise auf eine grundsätzliche Bedeutung der zu lösenden Rechtsfrage vor.

Es war daher spruchgemäß durch Senat zu entscheiden.