TE Bvwg Erkenntnis 2024/7/5 W292 2284228-1

JUSLINE Entscheidung

Veröffentlicht am 05.07.2024

Entscheidungsdatum

05.07.2024

Norm

B-VG Art133 Abs4
DSG §1
DSG §24
DSG §4
DSGVO Art15
DSGVO Art2
DSGVO Art32
DSGVO Art33
DSGVO Art34
DSGVO Art4
DSGVO Art5
DSGVO Art58
DSGVO Art6
DSGVO Art77
VwGVG §28 Abs2

1. B-VG Art. 133 heute
2. B-VG Art. 133 gültig von 01.01.2019 bis 24.05.2018zuletzt geändert durch BGBl. I Nr. 138/2017
3. B-VG Art. 133 gültig ab 01.01.2019zuletzt geändert durch BGBl. I Nr. 22/2018
4. B-VG Art. 133 gültig von 25.05.2018 bis 31.12.2018zuletzt geändert durch BGBl. I Nr. 22/2018
5. B-VG Art. 133 gültig von 01.08.2014 bis 24.05.2018zuletzt geändert durch BGBl. I Nr. 164/2013
6. B-VG Art. 133 gültig von 01.01.2014 bis 31.07.2014zuletzt geändert durch BGBl. I Nr. 51/2012
7. B-VG Art. 133 gültig von 01.01.2004 bis 31.12.2013zuletzt geändert durch BGBl. I Nr. 100/2003
8. B-VG Art. 133 gültig von 01.01.1975 bis 31.12.2003zuletzt geändert durch BGBl. Nr. 444/1974
9. B-VG Art. 133 gültig von 25.12.1946 bis 31.12.1974zuletzt geändert durch BGBl. Nr. 211/1946
10. B-VG Art. 133 gültig von 19.12.1945 bis 24.12.1946zuletzt geändert durch StGBl. Nr. 4/1945
11. B-VG Art. 133 gültig von 03.01.1930 bis 30.06.1934

1. DSG Art. 1 § 1 heute
2. DSG Art. 1 § 1 gültig ab 01.01.2014zuletzt geändert durch BGBl. I Nr. 51/2012
3. DSG Art. 1 § 1 gültig von 01.01.2000 bis 31.12.2013

1. DSG Art. 2 § 24 heute
2. DSG Art. 2 § 24 gültig ab 15.07.2024 zuletzt geändert durch BGBl. I Nr. 70/2024
3. DSG Art. 2 § 24 gültig von 25.05.2018 bis 14.07.2024 zuletzt geändert durch BGBl. I Nr. 120/2017
4. DSG Art. 2 § 24 gültig von 01.01.2010 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 133/2009
5. DSG Art. 2 § 24 gültig von 01.01.2000 bis 31.12.2009

1. DSG Art. 2 § 4 heute
2. DSG Art. 2 § 4 gültig ab 01.01.2020 zuletzt geändert durch BGBl. I Nr. 14/2019
3. DSG Art. 2 § 4 gültig von 25.05.2018 bis 31.12.2019 zuletzt geändert durch BGBl. I Nr. 24/2018
4. DSG Art. 2 § 4 gültig von 25.05.2018 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 120/2017
5. DSG Art. 2 § 4 gültig von 01.01.2010 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 133/2009
6. DSG Art. 2 § 4 gültig von 01.01.2000 bis 31.12.2009

1. VwGVG § 28 heute
2. VwGVG § 28 gültig ab 01.01.2019 zuletzt geändert durch BGBl. I Nr. 138/2017
3. VwGVG § 28 gültig von 01.01.2014 bis 31.12.2018

Spruch

W292 2284228-1/49E

IM NAMEN DER REPUBLIK!

Das Bundesverwaltungsgericht hat durch den Richter Mag. Herwig ZACZEK als Vorsitzenden und die fachkundigen Laienrichter, Mag. René BOGENDORFER und Mag. Thomas GSCHAAR als Beisitzer, über die Beschwerde der X GmbH (nunmehr Y GmbH), XXXX , vertreten durch die Schönherr Rechtsanwälte GmbH, Schottenring 19, 1010 Wien, gegen den Bescheid der Datenschutzbehörde vom 27.11.2023, Zl. D124.0960/23 / 2023-0.703.446 (mitbeteiligte Partei: XXXX , vertreten durch: RA Mag. Robert HAUPT und RA Mag. Dr. Florian SCHEIBER), nach Durchführung einer mündlichen Verhandlung am 28.02.2024 zu Recht erkannt:Das Bundesverwaltungsgericht hat durch den Richter Mag. Herwig ZACZEK als Vorsitzenden und die fachkundigen Laienrichter, Mag. René BOGENDORFER und Mag. Thomas GSCHAAR als Beisitzer, über die Beschwerde der römisch zehn GmbH (nunmehr Y GmbH), römisch 40 , vertreten durch die Schönherr Rechtsanwälte GmbH, Schottenring 19, 1010 Wien, gegen den Bescheid der Datenschutzbehörde vom 27.11.2023, Zl. D124.0960/23 / 2023-0.703.446 (mitbeteiligte Partei: römisch 40 , vertreten durch: RA Mag. Robert HAUPT und RA Mag. Dr. Florian SCHEIBER), nach Durchführung einer mündlichen Verhandlung am 28.02.2024 zu Recht erkannt:

A)

Die Beschwerde wird gemäß § 28 Abs. 2 VwGVG, § 1 und 24 DSG in Verbindung mit Art. 5, 6, 32 und 77 DSGVO, als unbegründet abgewiesen.Die Beschwerde wird gemäß Paragraph 28, Absatz 2, VwGVG, Paragraph eins und 24 DSG in Verbindung mit Artikel 5,, 6, 32 und 77 DSGVO, als unbegründet abgewiesen.

B)

Die Revision ist gemäß Art. 133 Abs. 4 B-VG nicht zulässigDie Revision ist gemäß Artikel 133, Absatz 4, B-VG nicht zulässig.

Text

Entscheidungsgründe:

I. Verfahrensgang:römisch eins. Verfahrensgang:

1. Mit dem verfahrenseinleitenden Antrag vom 19.04.2023, einer auf Art. 77 DSGVO und § 24 DSG gestützten Beschwerde an die Datenschutzbehörde, behauptete die mitbeteiligte Partei, durch die (nunmehrige) Beschwerdeführerin (Beschwerdegegnerin im Verfahren vor der belangten Behörde) in Rechten nach der DSGVO, konkret durch Verstöße gegen Datenverarbeitungsgrundsätze des Art. 5 Abs. 1 DSGVO und Benachrichtigungspflichten

nach Art. 34 DSGVO, sowie im Recht auf Geheimhaltung nach § 1 DSG verletzt worden zu sein.1. Mit dem verfahrenseinleitenden Antrag vom 19.04.2023, einer auf Artikel 77, DSGVO und Paragraph 24, DSG gestützten Beschwerde an die Datenschutzbehörde, behauptete die mitbeteiligte Partei, durch die (nunmehrige) Beschwerdeführerin (Beschwerdegegnerin im Verfahren vor der belangten Behörde) in Rechten nach der DSGVO, konkret durch Verstöße gegen Datenverarbeitungsgrundsätze des Artikel 5, Absatz eins, DSGVO und Benachrichtigungspflichten nach Artikel 34, DSGVO, sowie im Recht auf Geheimhaltung nach Paragraph eins, DSG verletzt worden zu sein.

Zusammengefasst brachte die mitbeteiligte Partei vor, ein „Hacker“ habe die Meldedaten fast aller Österreicher aus einer Datenbank der Verantwortlichen entwendet, diese habe nämlich mit einem IT-Dienstleister zusammengearbeitet, bei dem es zu Nachlässigkeiten gekommen sei, wodurch die Datenbank der Verantwortlichen im Mai 2020 ohne Zugangssicherung im Internet zugänglich gewesen wäre. Dies entspreche nicht den datenschutzrechtlichen Vorgaben hinsichtlich der Sicherheit der Verarbeitung personenbezogener Daten und sei das Fehlverhalten des IT-Dienstleisters der Verantwortlichen zuzurechnen. Zudem habe hinsichtlich der gegenständlichen Vorfälle keine individuelle Benachrichtigung im Sinne von Art. 34 DSGVO stattgefunden. Zusammengefasst brachte die mitbeteiligte Partei vor, ein „Hacker“ habe die Meldedaten fast aller Österreicher aus einer Datenbank der Verantwortlichen entwendet, diese habe nämlich mit einem IT-Dienstleister zusammengearbeitet, bei dem es zu Nachlässigkeiten gekommen sei, wodurch die Datenbank der Verantwortlichen im Mai 2020 ohne Zugangssicherung im Internet zugänglich gewesen wäre. Dies entspreche nicht den datenschutzrechtlichen Vorgaben hinsichtlich der Sicherheit der Verarbeitung personenbezogener Daten und sei das Fehlverhalten des IT-Dienstleisters der Verantwortlichen zuzurechnen. Zudem habe hinsichtlich der gegenständlichen Vorfälle keine individuelle Benachrichtigung im Sinne von Artikel 34, DSGVO stattgefunden.

2. Aufgrund einer Vielzahl gleichgelagerter Datenschutzbeschwerden, denen derselbe Sachverhalt zugrunde lag, führte die Datenschutzbehörde (belangte Behörde), protokolliert zur Zl. D124.0227/23, ein einheitliches Ermittlungsverfahren („Hauptverfahren“) durch, in Rahmen dessen setzte die belangte Behörde umfassende Ermittlungsschritte und legte die gewonnenen Ermittlungsergebnisse im Sinne der Verfahrensökonomie allen gegen die Verantwortliche gerichteten Verfahren zu Grunde.

3. Mit dem angefochtenen Bescheid hat die Datenschutzbehörde (belangte Behörde) der Datenschutzbeschwerde der mitbeteiligten Partei teilweise Folge gegeben und – soweit für das hg. Beschwerdeverfahren von Relevanz – festgestellt, die [Beschwerdeführerin] habe die [mitbeteiligte Partei] im Recht auf Geheimhaltung verletzt, indem die [Beschwerdeführerin] es mangels geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO („Sicherheit der Verarbeitung") ermöglicht habe, dass personenbezogene Daten der [mitbeteiligten Partei] (jedenfalls Vor- und Nachname, Geburtsdatum und postalische Anschrift) zumindest einer dritten Person (Hacker) unrechtmäßig zugänglich wurden. 3. Mit dem angefochtenen Bescheid hat die Datenschutzbehörde (belangte Behörde) der Datenschutzbeschwerde der mitbeteiligten Partei teilweise Folge gegeben und – soweit für das hg. Beschwerdeverfahren von Relevanz – festgestellt, die [Beschwerdeführerin] habe die [mitbeteiligte Partei] im Recht auf Geheimhaltung verletzt, indem die [Beschwerdeführerin] es mangels geeigneter technischer und organisatorischer Maßnahmen gemäß Artikel 32, DSGVO („Sicherheit der Verarbeitung") ermöglicht habe, dass personenbezogene Daten der [mitbeteiligten Partei] (jedenfalls Vor- und Nachname, Geburtsdatum und postalische Anschrift) zumindest einer dritten Person (Hacker) unrechtmäßig zugänglich wurden.

4. Gegen den oben bezeichneten Bescheid der Datenschutzbehörde richtet sich die verfahrensgegenständliche Bescheidbeschwerde.

Darin bringt die Beschwerdeführerin zusammengefasst zunächst vor, das Beschwerderecht der mitbeteiligten Partei sei im Sinne von § 24 Abs. 4 DSG präkludiert, da die mitbeteiligte Partei bereits seit dem Jahr 2020 Kenntnis von einer sie potenziell betreffenden Datenschutzverletzung gehabt habe, die verfahrenseinleitende Datenschutzbeschwerde jedoch erst im Jahre 2023 erhoben worden sei. Weiterhin rügt die Beschwerdeführerin ein in mehrfacher Hinsicht mangelhaft geführtes Ermittlungsverfahren sowie eine daraus resultierende unrichtige rechtliche Beurteilung. Zudem sei es mit 01.01.2024 zu einer Änderung der Rechtslage gekommen, wodurch die nunmehrige Y GmbH GmbH nicht (mehr) als für den verfahrensgegenständlichen Sicherheitsvorfall aus dem Jahr 2020 datenschutzrechtlich Verantwortliche angesehen werden könne.Darin bringt die Beschwerdeführerin zusammengefasst zunächst vor, das Beschwerderecht der mitbeteiligten Partei sei im Sinne von Paragraph 24, Absatz 4, DSG präkludiert, da die

mitbeteiligte Partei bereits seit dem Jahr 2020 Kenntnis von einer sie potenziell betreffenden Datenschutzverletzung gehabt habe, die verfahrenseinleitende Datenschutzbeschwerde jedoch erst im Jahre 2023 erhoben worden sei. Weiterhin rügt die Beschwerdeführerin ein in mehrfacher Hinsicht mangelhaft geführtes Ermittlungsverfahren sowie eine daraus resultierende unrichtige rechtliche Beurteilung. Zudem sei es mit 01.01.2024 zu einer Änderung der Rechtslage gekommen, wodurch die nunmehrige Y GmbH GmbH nicht (mehr) als für den verfahrensgegenständlichen Sicherheitsvorfall aus dem Jahr 2020 datenschutzrechtlich Verantwortliche angesehen werden könne.

5. Die belangte Behörde hat die gegenständliche Beschwerde samt den Bezug habenden Verwaltungsakten dem Bundesverwaltungsgericht vorgelegt, ohne von der Möglichkeit einer Beschwerdevorentscheidung Gebrauch zu machen.

6. Am 28.02.2024 fand vor dem Bundesverwaltungsgericht eine mündliche Beschwerdeverhandlung in der gegenständlichen Rechtssache statt. Im Rahmen der mündlichen Verhandlung wurde unter anderem der Geschäftsführer des IT-Dienstleisters der X als Zeuge einvernommen, im Beisein der Parteien und deren Rechtsvertretern Beweise im Wege der Einsichtnahme in die in Rede stehenden Datensätze aufgenommen sowie die Sach- und Rechtslage umfassend erörtert. 6. Am 28.02.2024 fand vor dem Bundesverwaltungsgericht eine mündliche Beschwerdeverhandlung in der gegenständlichen Rechtssache statt. Im Rahmen der mündlichen Verhandlung wurde unter anderem der Geschäftsführer des IT-Dienstleisters der römisch zehn als Zeuge einvernommen, im Beisein der Parteien und deren Rechtsvertretern Beweise im Wege der Einsichtnahme in die in Rede stehenden Datensätze aufgenommen sowie die Sach- und Rechtslage umfassend erörtert.

II. Das Bundesverwaltungsgericht hat erwogen:römisch II. Das Bundesverwaltungsgericht hat erwogen:

1. Feststellungen:

1.1. Die X GmbH (FN XXXX , im Folgenden auch: X GmbH) wurde laut Firmenbuch am 09.09.1998 errichtet und war unter diesem Firmenwortlaut bis zum 31.12.2023 mit der Einbringung und Abrechnung der Rundfunkgebühr in Österreich beauftragt und vollzog das Rundfunkgebührengesetz. Zur Wahrnehmung dieser Aufgabe erhielt sie Meldedaten aus lokalen Melderegistern von den jeweiligen lokalen Meldebehörden. Hierzu gehörten in der Regel zumindest der Vor- und Nachname, das Geburtsdatum und die postalische Anschrift von in Österreich gemeldeten Personen.1.1. Die römisch zehn GmbH (FN römisch 40 , im Folgenden auch: römisch zehn GmbH) wurde laut Firmenbuch am 09.09.1998 errichtet und war unter diesem Firmenwortlaut bis zum 31.12.2023 mit der Einbringung und Abrechnung der Rundfunkgebühr in Österreich beauftragt und vollzog das Rundfunkgebührengesetz. Zur Wahrnehmung dieser Aufgabe erhielt sie Meldedaten aus lokalen Melderegistern von den jeweiligen lokalen Meldebehörden. Hierzu gehörten in der Regel zumindest der Vor- und Nachname, das Geburtsdatum und die postalische Anschrift von in Österreich gemeldeten Personen.

1.2. Die Firma der X GmbH wurde mit Wirkung zum 01.01.2024 in Y GmbH (im Folgenden auch: Y GmbH) geändert. An den Eigentumsverhältnissen hat sich seit der Errichtung der Gesellschaft keine Änderung ergeben, als Alleingesellschafterin scheint im Firmenbuch zum Entscheidungszeitpunkt nach wie vor der XXXX (FN XXXX) auf. 1.2. Die Firma der römisch zehn GmbH wurde mit Wirkung zum 01.01.2024 in Y GmbH (im Folgenden auch: Y GmbH) geändert. An den Eigentumsverhältnissen hat sich seit der Errichtung der Gesellschaft keine Änderung ergeben, als Alleingesellschafterin scheint im Firmenbuch zum Entscheidungszeitpunkt nach wie vor der römisch 40 (FN römisch 40) auf.

1.3. Die X verfügte zur Erfüllung ihres gesetzlichen Auftrages über umfassende Datenbanken, die Meldedaten aller in Österreich gemeldeten Personen sowie Gebäudedaten umfasste (vgl. § 4 RGG). 1.3. Die römisch zehn verfügte zur Erfüllung ihres gesetzlichen Auftrages über umfassende Datenbanken, die Meldedaten aller in Österreich gemeldeten Personen sowie Gebäudedaten umfasste vergleiche Paragraph 4, RGG).

1.4. Im Vorfeld des Sicherheitsvorfalles vom Mai 2020 wurde von der X ein sogenanntes CRM-System (Customer-Relationship-Management System) entwickelt und eingeführt. Für die Umsetzung dieses IT-Projektes wurde ein IT-Dienstleistungsunternehmen, die Z Service GmbH (im Folgenden: „IT-Dienstleister“), herangezogen. Konkret wurde das IT-Unternehmen mit der Systemgestaltungsentwicklung und Implementierung einer Adressdatenbank zur Verwaltung von Meldedaten potenziell beitragspflichtiger Personen, diese Datenbank wird von X als „Adress-Master“ bezeichnet, beauftragt. Die X verfolgte mit diesem IT-Projekt das Ziel, eine Restrukturierung der Datenbestände (Meldedaten) zu erreichen, da die an die X von unterschiedlichen Meldebehörden (Städten und Gemeinden) gelieferten Meldedaten

eine nicht einheitliche Datenstruktur aufwiesen. Zwischen der X und dem IT-Dienstleister wurde hierzu eine (mit 13.09.2019 datierte) Vereinbarung unter Bezugnahme auf Art. 28 DSGVO geschlossen. 1.4. Im Vorfeld des Sicherheitsvorfalles vom Mai 2020 wurde von der römisch zehn ein sogenanntes CRM-System (Customer-Relationship-Management System) entwickelt und eingeführt. Für die Umsetzung dieses IT-Projektes wurde ein IT-Dienstleistungsunternehmen, die Z Service GmbH (im Folgenden: „IT-Dienstleister"), herangezogen. Konkret wurde das IT-Unternehmen mit der Systemgestaltungsentwicklung und Implementierung einer Adressdatenbank zur Verwaltung von Meldedaten potenziell beitragspflichtiger Personen, diese Datenbank wird von römisch zehn als „Adress-Master" bezeichnet, beauftragt. Die römisch zehn verfolgte mit diesem IT-Projekt das Ziel, eine Restrukturierung der Datenbestände (Meldedaten) zu erreichen, da die an die römisch zehn von unterschiedlichen Meldebehörden (Städten und Gemeinden) gelieferten Meldedaten eine nicht einheitliche Datenstruktur aufwiesen. Zwischen der römisch zehn und dem IT-Dienstleister wurde hierzu eine (mit 13.09.2019 datierte) Vereinbarung unter Bezugnahme auf Artikel 28, DSGVO geschlossen.

1.4.1. In dieser Vereinbarung heißt es auszugsweise wörtlich:

„... Die Firma Z Service GmbH , XXXX, XXXX, (im Folgenden: „Auftragnehmer") erbringt für die X GmbH, XXXX (im Folgenden: „Auftraggeber") dem in dem zwischen den beiden Parteien geschlossenen Leistungsvertrag (der „Vertrag") vertraglich festgeschriebenen Leistungen, welche die Verwendung personenbezogener, vom Auftraggeber an den Auftragnehmer überlassener Daten beinhalten. „... Die Firma Z Service GmbH , römisch 40 , römisch 40 , (im Folgenden: „Auftragnehmer") erbringt für die römisch zehn GmbH, römisch 40 (im Folgenden: „Auftraggeber") dem in dem zwischen den beiden Parteien geschlossenen Leistungsvertrag (der „Vertrag") vertraglich festgeschriebenen Leistungen, welche die Verwendung personenbezogener, vom Auftraggeber an den Auftragnehmer überlassener Daten beinhalten.

...

1. Verpflichtung zu nationalen und europäischen Datenschutzgesetzen und –normen

Der Auftragnehmer verpflichtet sich, die geltenden Datenschutzbestimmungen nach der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, kurz DSGVO) und den geltenden nationalen Gesetzen und Verordnung einzuhalten. Der Auftragnehmer ist verpflichtet, den Auftraggeber unverzüglich über gesetzliche Anforderungen und Änderungen zu informieren, die ihn von der Erfüllung dieses Vertrages behindern oder beschränken würden. In diesem Fall sind der Auftraggeber und der Auftragnehmer berechtigt, die weitere Ausführung des Vertrages auszusetzen und / oder vom Vertrag zurückzutreten.

Umfang, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der jeweiligen Vereinbarung beschrieben. Details und Spezifikationen der Verarbeitung personenbezogener Daten sind über den jeweiligen Vertrag oder ein Beiblatt zu dieser Vereinbarung geregelt.

...

Die Datenverarbeitung erfolgt ausschließlich in einem Mitgliedstaat der Europäischen Union. Jede Übertragung (einschließlich der Gewährung von Zugangsrechten oder der Nutzung von Unterstützungsdiensten) von einem Mitgliedstaat der Europäischen Union in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur dann durchgeführt werden, wenn zumindest die Anforderungen der Artikel 44 bis 50 DSGVO erfüllt sind.

...

4. Technische und organisatorische Maßnahmen

Der Auftragnehmer verpflichtet sich, alle notwendigen technischen und organisatorischen Maßnahmen nach den geltenden Datenschutzbestimmungen des Mitgliedstaats, der DSGVO und anderen anwendbaren nationalen Sonderregelungen zu treffen. ...

Die Datensicherheitsmaßnahmen müssen ein angemessenes Datenschutzniveau gewährleisten, insbesondere nach Art, Umfang, Umständen und Zweck der Datenverarbeitung sowie der Wahrscheinlichkeit des Auftretens und der Schwere der Risiken. Der Auftragnehmer verpflichtet sich sicherzustellen, dass die Datensicherheitsmaßnahmen dem

Stand der Technik entsprechen. Dies betrifft sowohl technische als auch organisatorische Maßnahmen (Vorgaben z.B. lt. ISO / IEC 27001 & 27002, sowie branchenüblichen Normane und Standards in der jeweils gültigen Version)."

6. Kontrollen und sonstige Verpflichtungen des Auftragnehmers

Der Auftragnehmer muss:

a) Aufzeichnungen über die Verarbeitung in Form und Stoff gemäß Art. 30 Abs. DSGVO führen;a) Aufzeichnungen über die Verarbeitung in Form und Stoff gemäß Artikel 30, Abs. DSGVO führen;

b) wenn gesetzlich vorgeschrieben, einen Datenschutzbeauftragten ernennen, der seine Aufgaben nach Art. 37 bis 39 DSGVO erfüllen kann und dem Auftraggeber die Kontaktdaten für die direkte Kommunikation zur Verfügung stellt; b) wenn gesetzlich vorgeschrieben, einen Datenschutzbeauftragten ernennen, der seine Aufgaben nach Artikel 37 bis 39 DSGVO erfüllen kann und dem Auftraggeber die Kontaktdaten für die direkte Kommunikation zur Verfügung stellt;

c) die personenbezogenen Daten und Daten der juristischen Personen vertraulich zu behandeln und nur Arbeitnehmer einzubeziehen, die sich verpflichtet haben, das Datengeheimnis zu beachten oder an die Berufsgeheimnisse gebunden sind, in jedem Fall bleiben die Geheimhaltungsplichten über das Ende des Vertrages hinaus gültig, diese Datenverarbeitungsvereinbarung oder den Arbeitsvertrag auf unbestimmte Zeit, unabhängig von der Bestimmung über andere Geheimhaltungspflichten

d) jede Person, die Zugang zu personenbezogenen Daten hat, über spezifische Datenschutzpflichten in Bezug auf diese Datenverarbeitungsvereinbarung sowie ihre Verpflichtungen zu Erfüllung von Weisungen und zur Nutzung personenbezogener Daten im Einklang mit dieser Datenverarbeitungsvereinbarung nachweislich informieren;

e) die für diese Datenverarbeitungsvereinbarung erforderlichen technischen und organisatorischen Maßnahmen umsetzen und einhalten sowie einem vom Auftraggeber bestimmten Auditor in diesem Zusammenhang verlangte Nachweise vorlegen;

f) eine Datenverletzung unverzüglich (innerhalb von 24 Stunden) melden, wenn dem Auftragnehmer eine Verletzung der personenbezogenen Daten, die der Datenverarbeitung unterliegen, gemäß dieser Datenverarbeitungsvereinbarung bewusst wird, um dem Auftraggeber die Erfüllung seiner „Datenverletzungsmittelung" gemäß Art. 33 DSGVO zu ermöglichen; f) eine Datenverletzung unverzüglich (innerhalb von 24 Stunden) melden, wenn dem Auftragnehmer eine Verletzung der personenbezogenen Daten, die der Datenverarbeitung unterliegen, gemäß dieser Datenverarbeitungsvereinbarung bewusst wird, um dem Auftraggeber die Erfüllung seiner „Datenverletzungsmittelung" gemäß Artikel 33, DSGVO zu ermöglichen;

g) den Auftraggeber von Kontrollmaßnahmen und Maßnahmen, die von einer Datenschutzaufsichtsbehörde oder anderen Untersuchungen durch eine Behörde über mögliche Verletzungen von Datenschutzgesetzen oder Fehlverhalten in dieser Hinsicht eingeleitet wurden, unverzüglich informieren.

7. Subauftragnehmer

Nach Art. 28 Abs. 2 DSGVO unterliegt die Beteiligung eines Subauftragnehmers einer gesonderten vorherigen schriftlichen Genehmigung des Auftraggebers. Folgende Mindest-Voraussetzungen müssen dabei erfüllt sein: Nach Artikel 28, Absatz 2, DSGVO unterliegt die Beteiligung eines Subauftragnehmers einer gesonderten vorherigen schriftlichen Genehmigung des Auftraggebers. Folgende Mindest-Voraussetzungen müssen dabei erfüllt sein:

a) Der Subauftragnehmer hat mindestens die gleichen technischen und organisatorischen Maßnahmen wie der Auftragnehmer zu erfüllen.

b) Der Auftragnehmer und der Subauftragnehmer haben eine vertragliche Vereinbarung abzuschließen, in der die gleichen Bedingungen für die Verarbeitung personenbezogener Daten festgelegt sind, wie zwischen Auftraggeber und Auftragnehmer.

c) Der Subauftragnehmer verpflichtet sich ebenfalls einer vom Auftraggeber beauftragten Person (Auditor) auf Verlangen sämtliche Nachweise zu technischen und organisatorischen Maßnahmen in Bezug auf die DSGVO und den Anforderungen der Informationssicherheit vorzulegen.

d) Bei der Datenverarbeitung eines Subauftragnehmers sind alle gemäß Art. 32 DSGVO erforderlichen Sicherheitsmaßnahmen zu treffen. Insbesondere dürfen für die Tätigkeit nur solche Mitarbeiterinnen / Mitarbeiter

herangezogen werden, die sich dem AV gegenüber zur Einhaltung des Datengeheimnisses gemäß § 15 DSG 2000 (Geheimhaltung von personenbezogenen Daten) bzw. der Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO) und über die einschlägigen strafrechtlichen Bestimmungen nachweislich informiert wurden. d) Bei der Datenverarbeitung eines Subauftragnehmers sind alle gemäß Artikel 32, DSGVO erforderlichen Sicherheitsmaßnahmen zu treffen. Insbesondere dürfen für die Tätigkeit nur solche Mitarbeiterinnen / Mitarbeiter herangezogen werden, die sich dem AV gegenüber zur Einhaltung des Datengeheimnisses gemäß Paragraph 15, DSG 2000 (Geheimhaltung von personenbezogenen Daten) bzw. der Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Artikel 28, Absatz 3, Litera b, DSGVO) und über die einschlägigen strafrechtlichen Bestimmungen nachweislich informiert wurden.

Ungeachtet der Ermächtigung des Auftraggebers bleibt der Auftragnehmer für die Einhaltung der Datenschutzpflichten des Subauftragnehmers verantwortlich. Wenn der Subauftragnehmer seinen Datenschutzanforderungen nicht nachkommt, haftet der Auftragnehmer für Subauftragnehmer.

..."

1.4.2. Der Projektauftrag der X umfasste die Entwicklung einer durchsuchbaren Software für einheitliche Meldedaten. Den Projektauftrag erteilte die X Anfang 2019 und war die Softwareentwicklung mit Testdaten bereits im Dezember 2019 abgeschlossen. Die tatsächliche Softwareentwicklung erfolgte über weite Teile durch eine serbische Tochtergesellschaft des IT-Dienstleisters, da der IT-Dienstleister zum damaligen Zeitpunkt in Österreich lediglich über zwei Mitarbeiter verfügte, wobei es sich bei einem der Mitarbeiter um den Gesellschaftergeschäftsführer selbst handelte. Zum fraglichen Zeitpunkt verfügte der IT-Dienstleister im Rahmen der serbischen Tochtergesellschaft über acht bis zehn Mitarbeiter. Im Rahmen der Neustrukturierung der Datenbanken war die X vollumfänglich in den Entwicklungs- und Umsetzungsprozess durch den IT-Dienstleister eingebunden. X war seit Projektbeginn bekannt, dass Softwareprogrammierer des serbischen Tochterunternehmens des IT-Dienstleisters in Serbien federführend an der Softwareentwicklung im Rahmen des in Rede stehenden Projektes arbeiteten. 1.4.2. Der Projektauftrag der römisch zehn umfasste die Entwicklung einer durchsuchbaren Software für einheitliche Meldedaten. Den Projektauftrag erteilte die römisch zehn Anfang 2019 und war die Softwareentwicklung mit Testdaten bereits im Dezember 2019 abgeschlossen. Die tatsächliche Softwareentwicklung erfolgte über weite Teile durch eine serbische Tochtergesellschaft des IT-Dienstleisters, da der IT-Dienstleister zum damaligen Zeitpunkt in Österreich lediglich über zwei Mitarbeiter verfügte, wobei es sich bei einem der Mitarbeiter um den Gesellschaftergeschäftsführer selbst handelte. Zum fraglichen Zeitpunkt verfügte der IT-Dienstleister im Rahmen der serbischen Tochtergesellschaft über acht bis zehn Mitarbeiter. Im Rahmen der Neustrukturierung der Datenbanken war die römisch zehn vollumfänglich in den Entwicklungs- und Umsetzungsprozess durch den IT-Dienstleister eingebunden. römisch zehn war seit Projektbeginn bekannt, dass Softwareprogrammierer des serbischen Tochterunternehmens des IT-Dienstleisters in Serbien federführend an der Softwareentwicklung im Rahmen des in Rede stehenden Projektes arbeiteten.

1.5. Von der X GmbH wurde dem IT-Dienstleister keine Testumgebung in Form von Server-Infrastruktur zur Verfügung gestellt. Der IT-Dienstleister richtete auf Aufforderung von X auf einem bereits Anfang 2019 angemieteten Cloud-Server eine Testumgebung ein. Anbieter des Cloud-Servers war eine Gesellschaft mit Sitz in Deutschland, die S GmbH , XXXX , Deutschland (IP: XXXX , Domäne: XXXX). Zugangsdaten zum Testserver wurden vom IT-Dienstleister auch der X zur Verfügung gestellt.1.5. Von der römisch zehn GmbH wurde dem IT-Dienstleister keine Testumgebung in Form von Server-Infrastruktur zur Verfügung gestellt. Der IT-Dienstleister richtete auf Aufforderung von römisch zehn auf einem bereits Anfang 2019 angemieteten Cloud-Server eine Testumgebung ein. Anbieter des Cloud-Servers war eine Gesellschaft mit Sitz in Deutschland, die S GmbH , römisch 40 , Deutschland (IP: römisch 40 , Domäne: römisch 40). Zugangsdaten zum Testserver wurden vom IT-Dienstleister auch der römisch zehn zur Verfügung gestellt.

1.6. Die X GmbH hat zwischen dem 01.05.2020 und 05.05.2020 personenbezogene Daten über eine Datenaustauschplattform in Gestalt von Meldedaten aus der Meldedatenbank der X GmbH im Ausmaß von zumindest fünf bis sechs Millionen Datensätzen dem IT-Dienstleister bereitgestellt. Diese Daten wurden vom IT-Dienstleister am 06.05.2020 auf den angemieteten Test-Server in Deutschland geladen. Auf diese Testumgebung griffen sowohl Mitarbeiter des IT-Dienstleisters als auch der X per Fernzugriff (Remote-Access) zu. Der IT-Dienstleister hat die seitens der X GmbH zur Verfügung gestellten Daten — im Wesentlichen Meldedaten — auf eine Testumgebung geladen. Grundlage für die Testumgebung war der sog. Elastic Stack (ELK Stack). „ELK" ist die Abkürzung für drei Open-Source-

Projekte: Elasticsearch, Logstash und Kibana. Im Rahmen der Einführung eines zentralen Adressverwaltungs-Systems wurde zumindest „Elasticsearch" zur Abfrage der normalisierten Meldedaten verwendet.1.6. Die römisch zehn GmbH hat zwischen dem 01.05.2020 und 05.05.2020 personenbezogene Daten über eine Datenaustauschplattform in Gestalt von Meldedaten aus der Meldedatenbank der römisch zehn GmbH im Ausmaß von zumindest fünf bis sechs Millionen Datensätzen dem IT-Dienstleister bereitgestellt. Diese Daten wurden vom IT-Dienstleister am 06.05.2020 auf den angemieteten Test-Server in Deutschland geladen. Auf diese Testumgebung griffen sowohl Mitarbeiter des IT-Dienstleisters als auch der römisch zehn per Fernzugriff (Remote-Access) zu. Der IT-Dienstleister hat die seitens der römisch zehn GmbH zur Verfügung gestellten Daten — im Wesentlichen Meldedaten — auf eine Testumgebung geladen. Grundlage für die Testumgebung war der sog. Elastic Stack (ELK Stack). „ELK" ist die Abkürzung für drei Open-Source-Projekte: Elasticsearch, Logstash und Kibana. Im Rahmen der Einführung eines zentralen Adressverwaltungs-Systems wurde zumindest „Elasticsearch" zur Abfrage der normalisierten Meldedaten verwendet.

1.7. Ein Mitarbeiter des IT-Dienstleisters, der an dem in Rede stehenden IT-Projekt im Mai 2020 arbeitete, erfuhr am 27.05.2020 aus den Medien von einem externen widerrechtlichen Zugriff und befürchtete, dass es sich um die von X zur Verfügung gestellten Meldedaten handelte. Im Rahmen der Überprüfung durch den Mitarbeiter stellte sich heraus, dass eine technische Sicherheitslücke an dem zu Testzwecken genutzten Server bestand, dies in Gestalt einer offenen – aus dem öffentlichen Internet erreichbaren – Netzwerkschnittstelle, dem TCP Port 9200, unbekannte Täter diese Sicherheitslücke ausgenutzt und die dort gespeicherten Meldedaten bereits am 08.05.2020 abgegriffen haben. Der unrechtmäßige externe Zugriff auf den Meldedatenbestand konnte durch Auswertung von Protokolldaten (Log-Files) am Server festgestellt werden. Ermöglicht wurde der unrechtmäßige externe Zugriff dadurch, dass ein kurzzeitig für das Unternehmen tätiger Mitarbeiter des IT-Dienstleisters im Rahmen von Entwicklungs- bzw. Testtätigkeiten den TCP-Port 9200 zum Testserver in Deutschland offengelassen hat und die dort betriebene Meldedatenbank nicht durch ein Benutzerauthentifizierungssystem (bspw. Benutzername und Kennwort) vor unrechtmäßigen Zugriffen geschützt war. Der betreffende TCP-Port 9200 wurde im Vorfeld des widerrechtlichen externen Zugriffs vom 08.05.2020 seit Dezember 2019 immer wieder geöffnet und geschlossen. Der betreffende Mitarbeiter des IT-Dienstleisters verfügte auf dem Test-Server in Deutschland über die erforderlichen Zugriffsrechte, um dort entsprechende Konfigurationen vorzunehmen, hat das Unternehmen jedoch bereits vor Mai 2020 verlassen. Welche genauen Anweisungen dieser Mitarbeiter von ihm vorgesetzten Personen des IT-Dienstleisters erhalten hat und weshalb es erforderlich war, dass dieser Mitarbeiter derart umfangreiche Konfigurationsrechte in Bezug auf den Test-Server hatte, konnte nicht festgestellt werden. Ob und wann die auf dem betroffenen Server befindlichen personenbezogenen Daten der Adressdatenbank endgültig gelöscht wurden, kann nicht festgestellt werden. 1.7. Ein Mitarbeiter des IT-Dienstleisters, der an dem in Rede stehenden IT-Projekt im Mai 2020 arbeitete, erfuhr am 27.05.2020 aus den Medien von einem externen widerrechtlichen Zugriff und befürchtete, dass es sich um die von römisch zehn zur Verfügung gestellten Meldedaten handelte. Im Rahmen der Überprüfung durch den Mitarbeiter stellte sich heraus, dass eine technische Sicherheitslücke an dem zu Testzwecken genutzten Server bestand, dies in Gestalt einer offenen – aus dem öffentlichen Internet erreichbaren – Netzwerkschnittstelle, dem TCP Port 9200, unbekannte Täter diese Sicherheitslücke ausgenutzt und die dort gespeicherten Meldedaten bereits am 08.05.2020 abgegriffen haben. Der unrechtmäßige externe Zugriff auf den Meldedatenbestand konnte durch Auswertung von Protokolldaten (Log-Files) am Server festgestellt werden. Ermöglicht wurde der unrechtmäßige externe Zugriff dadurch, dass ein kurzzeitig für das Unternehmen tätiger Mitarbeiter des IT-Dienstleisters im Rahmen von Entwicklungs- bzw. Testtätigkeiten den TCP-Port 9200 zum Testserver in Deutschland offengelassen hat und die dort betriebene Meldedatenbank nicht durch ein Benutzerauthentifizierungssystem (bspw. Benutzername und Kennwort) vor unrechtmäßigen Zugriffen geschützt war. Der betreffende TCP-Port 9200 wurde im Vorfeld des widerrechtlichen externen Zugriffs vom 08.05.2020 seit Dezember 2019 immer wieder geöffnet und geschlossen. Der betreffende Mitarbeiter des IT-Dienstleisters verfügte auf dem Test-Server in Deutschland über die erforderlichen Zugriffsrechte, um dort entsprechende Konfigurationen vorzunehmen, hat das Unternehmen jedoch bereits vor Mai 2020 verlassen. Welche genauen Anweisungen dieser Mitarbeiter von ihm vorgesetzten Personen des IT-Dienstleisters erhalten hat und weshalb es erforderlich war, dass dieser Mitarbeiter derart umfangreiche Konfigurationsrechte in Bezug auf den Test-Server hatte, konnte nicht festgestellt werden. Ob und wann die auf dem betroffenen Server befindlichen personenbezogenen Daten der Adressdatenbank endgültig gelöscht wurden, kann nicht festgestellt werden.

1.8. Einem Dritten (in der Folge auch: „Hacker“) gelang es im Mai 2020 durch gezielte Suchen die Ziel-IP-Adresse und den Ziel-Port des Servers der Testumgebung, auf dem die Meldedaten von X vorhanden waren, konkret: der

verfahrensgegenständlichen Elastic Search Umgebung, herauszufinden. Danach gelang es dem Hacker, über den offenen TCP-Port 9200 auf die dort gespeicherte Meldedatenbank zuzugreifen und den Datenbestand zu exfiltrieren. Durch den offenen TCP-Port 9200 war es für den Zugriff auf die (Melde-)Datenbank nicht erforderlich, sich mittels Fernzugriffsverbindung (Remote-Access) mit dem Server der Testumgebung zu verbinden. Vorkehrungen bzw. Sicherheitsmechanismen, um einen unautorisierten Zugriff auf die (Melde-)Datenbank zu verhindern, wie etwa eine zusätzliche Zugangsbeschränkung durch Authentifizierung mittels Benutzername und Kennwort, waren im Rahmen der Konfiguration und Inbetriebnahme des Testservers seitens des IT-Dienstleisters (in Bezug auf die dort gespeicherten Meldedaten) nicht getroffen worden.1.8. Einem Dritten (in der Folge auch: „Hacker“) gelang es im Mai 2020 durch gezielte Suchen die Ziel-IP-Adresse und den Ziel-Port des Servers der Testumgebung, auf dem die Meldedaten von römisch zehn vorhanden waren, konkret: der verfahrensgegenständlichen Elastic Search Umgebung, herauszufinden. Danach gelang es dem Hacker, über den offenen TCP-Port 9200 auf die dort gespeicherte Meldedatenbank zuzugreifen und den Datenbestand zu exfiltrieren. Durch den offenen TCP-Port 9200 war es für den Zugriff auf die (Melde-)Datenbank nicht erforderlich, sich mittels Fernzugriffsverbindung (Remote-Access) mit dem Server der Testumgebung zu verbinden. Vorkehrungen bzw. Sicherheitsmechanismen, um einen unautorisierten Zugriff auf die (Melde-)Datenbank zu verhindern, wie etwa eine zusätzliche Zugangsbeschränkung durch Authentifizierung mittels Benutzername und Kennwort, waren im Rahmen der Konfiguration und Inbetriebnahme des Testservers seitens des IT-Dienstleisters (in Bezug auf die dort gespeicherten Meldedaten) nicht getroffen worden.

1.9. Zumindest ein Dritter (um wen es sich dabei konkret handelte, kann nicht festgestellt werden), hat den exfiltrierten Meldedatenbestand, also jene Meldedaten, die von X dem IT-Dienstleister im Mai 2020 zur Verfügung gestellt wurden, in Folge öffentlich im Internet, im sogenannten „RaidForums", zumindest im Mai 2020 zum Verkauf angeboten.1.9. Zumindest ein Dritter (um wen es sich dabei konkret handelte, kann nicht festgestellt werden), hat den exfiltrierten Meldedatenbestand, also jene Meldedaten, die von römisch zehn dem IT-Dienstleister im Mai 2020 zur Verfügung gestellt wurden, in Folge öffentlich im Internet, im sogenannten „RaidForums", zumindest im Mai 2020 zum Verkauf angeboten.

Der zum Kauf angebotene Meldedatenbestand wurde von einer öffentlichen Stelle in Österreich zwischen 24.05.2020 und 25.05.2020 angekauft.

1.10. Personenbezogene Daten der mitbeteiligten Partei, die X im Rahmen deren Meldedatenbank im Jahr 2019 verarbeitete, waren in dem Datenbestand, der von einem Dritten (Hacker) von dem Test-Server des IT-Dienstleisters in Deutschland am 08.05.2020 abgegriffen und in Folge zum Verkauf angeboten wurde, enthalten. 1.10. Personenbezogene Daten der mitbeteiligten Partei, die römisch zehn im Rahmen deren Meldedatenbank im Jahr 2019 verarbeitete, waren in dem Datenbestand, der von einem Dritten (Hacker) von dem Test-Server des IT-Dienstleisters in Deutschland am 08.05.2020 abgegriffen und in Folge zum Verkauf angeboten wurde, enthalten.

Konkret stellt sich der Datensatz hinsichtlich der mitbeteiligten Partei wie folgt dar:

Search " XXXX " (1 hit in 1 file of 5 searched)Search " römisch 40 " (1 hit in 1 file of 5 searched)

aus data_5.csv (1 hit)

Line 1322173:

MSc,6772324„ 2019/12/02,2018/10/03, H,2, XXXX , M,,, XXXX „ XXXX „Top XXXX , XXXX ,2,1„6800,17187,0003, XXXX ,044425, XXXX , XXXX MSc,6772324„ 2019/12/02,2018/10/03, H,2, römisch 40 , M,,, römisch 40 „ römisch 40 „Top römisch 40 , römisch 40 ,2,1„6800,17187,0003, römisch 40 ,044425, römisch 40 , römisch 40

1.11. Der Geschäftsführer der Z Service GmbH hat die Geschäftsführung der X GmbH zwischen 27.05.2020 und 28.05.2020 per E-Mail schriftlich von den unter 1.7. beschriebenen Vorgängen in Kenntnis gesetzt. 1.11. Der Geschäftsführer der Z Service GmbH hat die Geschäftsführung der römisch zehn GmbH zwischen 27.05.2020 und 28.05.2020 per E-Mail schriftlich von den unter 1.7. beschriebenen Vorgängen in Kenntnis gesetzt.

1.12. Personenbezogene Daten aus dem Meldedatenbestand der X verarbeitete der IT-Dienstleister bereits seit November 2019. Die am 08.05.2020 widerrechtlich abgegriffenen Daten waren jedoch erst seit wenigen Tagen vor dem 08.05.2020 im Besitz des IT-Dienstleisters.1.12. Personenbezogene Daten aus dem Meldedatenbestand der römisch zehn verarbeitete der IT-Dienstleister bereits seit November 2019. Die am 08.05.2020 widerrechtlich abgegriffenen Daten waren jedoch erst seit wenigen Tagen vor dem 08.05.2020 im Besitz des IT-Dienstleisters.

1.13. Am 27.05.2020 unterrichtete die X die Austria Presse Agentur (APA) über den verfahrensgegenständlichen Sicherheitsvorfall. Das hierzu an die APA versandte E-Mail der X konnte von der Beschwerdeführerin als Beweismittel im Verfahren vor dem BVwG nicht in Vorlage gebracht werden. Die Formulierung des Wortlauts der an die APA zu diesem Zweck übermittelten Nachricht erfolgte unter Einbindung der Kommunikationsabteilung des XXXX , die Textierung der diesbezüglich veröffentlichten APA-Meldung lautet wörtlich wie folgt [Formatierung nicht wie im Original]:1.13. Am 27.05.2020 unterrichtete die römisch zehn die Austria Presse Agentur (APA) über den verfahrensgegenständlichen Sicherheitsvorfall. Das hierzu an die APA versandte E-Mail der römisch zehn konnte von der Beschwerdeführerin als Beweismittel im Verfahren vor dem BVwG nicht in Vorlage gebracht werden. Die Formulierung des Wortlauts der an die APA zu diesem Zweck übermittelten Nachricht erfolgte unter Einbindung der Kommunikationsabteilung des römisch 40 , die Textierung der diesbezüglich veröffentlichten APA-Meldung lautet wörtlich wie folgt [Formatierung nicht wie im Original]:

„APA0488 5 II 0348 MI/CI Mi, 27.Mai 2020„APA0488 5 römisch II 0348 MI/CI Mi, 27.Mai 2020

Medien/Datenschutz/Ermittlung/Österreich

Verdacht auf Datendiebstahl bei X Verdacht auf Datendiebstahl bei römisch zehn

Utl.: Bundeskriminalamt und Verfassungsschutz ermitteln

Wien (APA) - Die XXXX -Tochter X (X) könnte von einem Datendiebstahl betroffen sein. Wie die für die Abwicklung der Rundfunkgebühren zuständige Firma der APA sagte, laufen derzeit Ermittlungen der Behörden dazu. Anlass sind dem Vernehmen nach auf einem Darknet-Marktplatz angebotene österreichische Daten, deren Zusammensetzung auf die von der X gespeicherten Informationen hinweist.Wien (APA) - Die römisch 40 -Tochter römisch zehn (römisch zehn) könnte von einem Datendiebstahl betroffen sein. Wie die für die Abwicklung der Rundfunkgebühren zuständige Firma der APA sagte, laufen derzeit Ermittlungen der Behörden dazu. Anlass sind dem Vernehmen nach auf einem Darknet-Marktplatz angebotene österreichische Daten, deren Zusammensetzung auf die von der römisch zehn gespeicherten Informationen hinweist.

"Wie heute bekannt wurde, dürfte es zu einem Diebstahl von größeren Mengen an Daten gekommen sein, wobei nicht ausgeschlossen werden kann, dass diese Daten aus dem Einflussbereich der X stammen", hieß es in einer schriftlichen Stellungnahme der X gegenüber der APA. Geschäftsführer XXXX betont, mit den Behörden zusammenzuarbeiten und die Systeme der X für Überprüfungen zur Verfügung gestellt zu haben. "Wie uns unsere Datenschutzexperten versichern, ist es seitens der X zu keinerlei Versäumnissen gekommen. Dies wird auch durch die im Februar erneuerte ISO-Zertifizierung der X -IT-Systeme untermauert", betonte XXXX ."Wie heute bekannt wurde, dürfte es zu einem Diebstahl von größeren Mengen an Daten gekommen sein, wobei nicht ausgeschlossen werden kann, dass diese Daten aus dem Einflussbereich der römisch zehn stammen", hieß es in einer schriftlichen Stellungnahme der römisch zehn gegenüber der APA. Geschäftsführer römisch 40 betont, mit den Behörden zusammenzuarbeiten und die Systeme der römisch zehn für Überprüfungen zur Verfügung gestellt zu haben. "Wie uns unsere Datenschutzexperten versichern, ist es seitens der römisch zehn zu keinerlei Versäumnissen gekommen. Dies wird auch durch die im Februar erneuerte ISO-Zertifizierung der römisch zehn -IT-Systeme untermauert", betonte römisch 40 .

"Das Bundeskriminalamt geht seit kurzem dem Verdacht eines Datendiebstahls nach", bestätigte Sprecher XXXX auf APA-Anfrage. Geführt werden die Ermittlungen demnach vom Cyber Crime Competence Center (C4) des Bundeskriminalamts mit Unterstützung des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT). Man arbeite eng mit der X zusammen."Das Bundeskriminalamt geht seit kurzem dem Verdacht eines Datendiebstahls nach", bestätigte Sprecher römisch 40 auf APA-Anfrage. Geführt werden die Ermittlungen demnach vom Cyber Crime Competence Center (C4) des Bundeskriminalamts mit Unterstützung des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT). Man arbeite eng mit der römisch zehn zusammen.

Wie viele Personen von dem möglichen Datendiebstahl betroffen sind und um welche Daten es sich genau handelt, war vorerst nicht zu erfahren. Anlass für die Ermittlungen war dem Vernehmen nach, dass auf einem Darknet-Marktplatz Daten angeboten wurden, deren Zusammensetzung auf die (teils aus dem Zentralen Melderegister abgefragten, Anm.) Kundendaten der X hinweist. Offiziell bestätigt wurde das allerdings nicht. Der NEOS-Abgeordnete XXXX hatte zuvor von einem einschlägigen Darkent-Angebot berichtet, auf dem behauptet wird, Adressen, Telefonnummern und Kontodaten von österreichischen Beamten, Richtern, Staatsanwälten und Journalisten zu verkaufen. Ob es sich dabei um jene Plattform handelt, die auch die aktuellen Ermittlungen ausgelöst hat, war vorerst

unklar. XXXX hielt auf Anfrage der APA auch einen Zusammenhang mit dem "Ergänzungsregister" auf der Seite des Wirtschaftsministeriums für möglich und forderte Aufklärung darüber, ob hier Daten abgeflossen sein könnten.“Wie viele Personen von dem möglichen Datendiebstahl betroffen sind und um welche Daten es sich genau handelt, war vorerst nicht zu erfahren. Anlass für die Ermittlungen war dem Vernehmen nach, dass auf einem Darknet-Marktplatz Daten angeboten wurden, deren Zusammensetzung auf die (teils aus dem Zentralen Melderegister abgefragten, Anmerkung Kundendaten der römisch zehn hinweist. Offiziell bestätigt wurde das allerdings nicht. Der NEOS-Abgeordnete römisch 40 hatte zuvor von einem einschlägigen Darkent-Angebot berichtet, auf dem behauptet wird, Adressen, Telefonnummern und Kontodaten von österreichischen Beamten, Richtern, Staatsanwälten und Journalisten zu verkaufen. Ob es sich dabei um jene Plattform handelt, die auch die aktuellen Ermittlungen ausgelöst hat, war vorerst unklar. römisch 40 hielt auf Anfrage der APA auch einen Zusammenhang mit dem "Ergänzungsregister" auf der Seite des Wirtschaftsministeriums für möglich und forderte Aufklärung darüber, ob hier Daten abgeflossen sein könnten.“

Diese APA-Meldung war auch auf der Homepage der X im Zeitraum von 27.05.2020, 17:16 Uhr, bis (inklusive) 14.12.2023, 14:20 Uhr, abrufbar.Diese APA-Meldung war auch auf der Homepage der römisch zehn im Zeitraum von 27.05.2020, 17:16 Uhr, bis (inklusive) 14.12.2023, 14:20 Uhr, abrufbar.

Zudem wurde der Wortlaut der APA-Meldung auch den Mitarbeitern des Kundendienstes der X zum Zweck der Beantwortung telefonischer Anfragen zur Verfügung gestellt. Der Inhalt der APA-Mitteilung wurde von zahlreichen Medienunternehmen im Mai 2020 aufgegriffen und in Kurzberichten thematisiert.Zudem wurde der Wortlaut der APA-Meldung auch den Mitarbeitern des Kundendienstes der römisch zehn zum Zweck der Beantwortung telefonischer Anfragen zur Verfügung gestellt. Der Inhalt der APA-Mitteilung wurde von zahlreichen Medienunternehmen im Mai 2020 aufgegriffen und in Kurzberichten thematisiert.

1.14. Eine individuelle Benachrichtigung einzelner potenziell von dem Sicherheitsvorfall betroffener Personen seitens der X hat zu keinem Zeitpunkt stattgefunden.1.14. Eine individuelle Benachrichtigung einzelner potenziell von dem Sicherheitsvorfall betroffener Personen seitens der römisch zehn hat zu keinem Zeitpunkt stattgefunden.

Die X GmbH hat selbst noch im Jahr 2023 auf Anträge auf Auskunft nach Art. 15 DSGVO, die sich auf den gegenständlichen Sicherheitsvorfall vom Mai 2020 bezogen haben mitgeteilt, dass sie keine Kenntnis über die jeweilige individuelle Betroffenheit der Antragsteller habe, und daher keine Auskunft darüber erteilen könne.Die römisch zehn GmbH hat selbst noch im Jahr 2023 auf Anträge auf Auskunft nach Artikel 15, DSGVO, die sich auf den gegenständlichen Sicherheitsvorfall vom Mai 2020 bezogen haben mitgeteilt, dass sie keine Kenntnis über die jeweilige individuelle Betroffenheit der Antragsteller habe, und daher keine Auskunft darüber erteilen könne.

1.15. Im Rahmen einer Meldung im Sinne von Art. 33 DSGVO an die Datenschutzbehörde vom 29.05.2020 führte die X in Bezug auf den Sicherheitsvorfall vom 08.05.2020 auszugsweise aus wie folgt [Formatierung nicht wie im Original, Unterstreichungen durch das Bundesverwaltungsgericht]: 1.15. Im Rahmen einer Meldung im Sinne von Artikel 33, DSGVO an die Datenschutzbehörde vom 29.05.2020 führte die römisch zehn in Bezug auf den Sicherheitsvorfall vom 08.05.2020 auszugsweise aus wie folgt [Formatierung nicht wie im Orig