Joachim Lindenberg
Heubergstraße 1a, 76228 Karlsruhe, Telefon 0721 98614618

Joachim Lindenberg, Heubergstraße 1a, 76228 Karlsruhe

Verwaltungsgericht Stuttgart

Telefax 0711 6673-6801

VG S 14 K 6288/24

Karlsruhe, den 16.12.2024

Sehr geehrte [redacted], sehr geehrter [redacted],
sehr geehrte Damen und Herren,

der Kläger stellt die zusätzlichen Anträge:

3. den Bescheid vom 06.12.2024 im Verfahren 4-0554.1-124/102 für nichtig zu erklären, hilfsweise aufzuheben, und den Beklagten anzuweisen, der Beschwerde in angemessenem Umfang nachzugehen und den Bescheid unter Berücksichtigung der Rechtsauffassung des Gerichts erneut zu erlassen,
4. beim Beklagten die vollständige Verwaltungsakte mit aktuellem Stand anzufordern und dem Kläger Akteneinsicht in die zu übermittelnden Verwaltungsakten zu gewähren.

Die verantwortliche Verivox GmbH – im Folgenden „Verantwortliche" ist beizuladen.

Begründung:

Der Bescheid vom 06.12.2024 erging erneut (vgl. 14 K 6171/24) ohne Anhörung des Klägers nach §28 LVwVfG BW und ist damit rechtswidrig ergangen.

Der Beklagte hat aber auch besonders schlampig ermittelt und bewertet, und damit auch gegen §24 LVwVfG BW verstoßen. Er hat lediglich Stellungnahmen der Verantwortlichen eingeholt, diese aber nicht ernsthaft überprüft. Aus Sicht des Klägers hat schon die Sachverhaltsermittlung viele Mängel:

- Der Beklagte schreibt: „Weitergehende, überprüfbare Nachweise für Ihre Vermutung haben Sie nicht vorgelegt." Nicht der Kläger sondern die Verantwortliche ist nach Art. 5 Abs. 2 i.V. mit Art. 5 Abs. 1 lit. f i.V.m. Art. 32 DSGVO rechenschafts- und damit beweispflichtig für die Sicherheit der Verarbeitung, und damit für die Unmöglichkeit des Daten-Leaks (vgl. EuGH vom 24.02.2022 C-175/20, Rn. 77 und Rn. 81; EuGH Urteil vom 04.05.2023 C-60/22 Rn. 53; BVerwG Urteil vom 02.03.2022, 6 C 7.20, Rn. 50). Dieser Beweis ist der Verantwortlichen wie der Kläger unten ausführen wird nicht gelungen.
- Der Beklagte hat in seinem Schreiben an die Verantwortliche vom 07.11.2024 nur zwei der vom Kläger als wahrscheinlich-geleakt gemeldeten Adressen angefragt (Bescheid Anlage 2, Rn. 6). Erfreulicherweise hat die Verantwortliche weitere berücksichtigt, aber nur insgesamt sechs von zehn tatsächlich bei Verivox verwendeten Emailadressen.

- Die Verantwortliche schreibt „Die Datenverarbeitung hängt von der jeweiligen Produktkategorie ab“ ohne konkret auszuführen wie (Bescheid Anlage 1, 2.2).
- Die Behauptung „Nach Abschluss dieser Überprüfung kann Verivox weiterhin belastbar ausschließen, dass die beiden E-Mail-Adressen widerrechtlich von den Systemen von Verivox abgeflossen sind (insbesondere nicht im Rahmen des MOVEit-Vorfalls).“ (Bescheid Anlage 2, Rn. 7) ist angesichts der mangelhaften Untersuchung des Vorfalls nicht haltbar. Zur Untersuchung (Bescheid Anlage 2, Rn. 8ff) darf der Kläger ausführen:
    - Die durch den Vorfall bekanntgewordene Schwachstelle CVE-2023-34362 war in allen Versionen von MOVEit mindestens seit 2019 bis zum Vorfall enthalten, also über fünf Jahre („All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions“ – Anlage K4 Mitre). Die Angreifer hatten also möglicherweise sehr lange Daten abgegriffen bevor die Schwachstelle bekannt wurde.
    - Die Schwachstelle CVE-2023-34362 erlaubt auch das Löschen von Daten („execute SQL statements that alter or delete database elements“ – Anlage K4 Mitre), es ist also nicht sichergestellt, dass die für die Untersuchung genutzte Kopie die abgegriffenen Daten überhaupt noch enthielt. Zumindest hätte die Verantwortliche darzustellen, wie sie das ausschließen kann. Oder im Umkehrschluss: es erscheint daher möglich, dass alle Daten die je über MOVEit übertragen wurden auch kompromittiert wurden. Damit wird die Aussage in Bescheid Anlage 1 unter 3. a) „Die gegenständlichen zwei E-Mail-Adressen sind vom Move-IT-Fall nicht betroffen, da diese Daten in Move-IT nicht enthalten sind“ fragwürdig. Ist hier gemeint, sie wurden in der forensischen Kopie nicht gefunden oder haben nie den Weg über MOVEit angetreten?
    - Dass nicht alle Attribute über MOVEit übertragen wurden (Rn. 10 ist irreführend, denn in allen dem Kläger bekannten Fällen waren Emailadresse und Bankverbindung an den Vertragspartner weitergegeben worden. Die Verantwortliche hat nicht dargestellt, dass diese Weitergabe nicht über MOVEit stattfand.
    - Die angeblich dem Stand der Technik entsprechenden Sicherheitsmaßnahmen (Rn. 13) entsprechen nicht dem Stand-der-Technik. Eine Firewall oder Verschlüsselung ist nicht geeignet eine SQL-Injection zu verhindern. Dazu bedarf es Softwareentwickler, die wissen was zu tun ist, und die Verantwortliche hätte dies und eine entsprechende Qualitätssicherung in die Verträge mit ihren Zuliefern aufnehmen müssen.
    - Unverständlich bleibt auch, wieso man eine Software verwendet, die keine Authentifizierung und damit auch keine Berechtigungsprüfung vorsieht (vgl. „that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database“ – Anlage K4 Mitre).
    - Nicht thematisiert wurde von der Verantwortlichen, ob es ein Löschkonzept für MOVEit gab, das den Umfang der über die Schwachstelle abgreifbaren Daten auf die Daten reduziert, die für noch offene Aufträge relevant sind. Historische Daten in einem über das Internet erreichbaren System zu speichern ist ein vermeidbares Risiko.
    - Nach www.verivox.de hat niemand gefragt.
- Es erstaunt bei der mangelhaften Untersuchung nicht, dass man ein Ablenkungsmanöver im Sinne von „Angriff ist die beste Verteidigung“ versucht (Bescheid Anlage 2 Rn. 14ff):

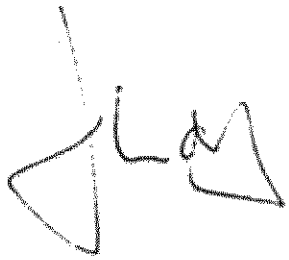
- Der Kläger und auch seine Kunden haben keinerlei Anhaltspunkte dafür, dass seine Sicherheit unzureichend ist (Rn. 14). Das Argument ist aber auch abwegig, denn über Verivox gab es offensichtlich viele weitere Beschwerden (Rn. 16), die Verivox mit der mangelhaften Untersuchung nicht nachvollziehen konnte oder wollte. Jedenfalls kann der Kläger versichern, dass es bei ihm im Unterschied zur Verantwortlichen mit Ausnahme der öffentlichen Webseiten, des öffentlichen DNS und von SMTP-Ports keine über das Internet erreichbaren Dienste gibt, die keine Authentifizierung erwarten.
- Auch Veröffentlichungen auf dem Blog des Kläger sind nicht die Ursache. Mit Ausnahme des Impressums werden seine Emailadressen dort per Software automatisch geschwärzt, lediglich zwischen dem 06.11.2024 und dem 12.12.2024 hat der Kläger dafür eine Ausnahme gemacht, weil der Beklagte anders nicht auf für den Sachverhalt wesentliche Informationen zugreifen konnte. Diese Seite war nicht in der Navigation enthalten und damit für Suchmaschinen nicht zu finden.
- Was will die Verantwortliche mit der Frage, ob der Kläger seine Mailboxen dokumentiere, aussagen? Der Kläger verwendet ein Catch-All, das ist zwar umstritten, erfüllt seine Anforderungen aber sehr gut. Insbesondere kann er feststellen, dass er genau drei Ursachen für Spam hat: öffentliche Adressen wie die im Impressum, unerwünschte Werbung von Geschäftspartnern, und Spam auf den Adressen, die in einer Verivox-Bestellung verwendet wurden.
- Mit dem Argument in Rn. 17 müsste der Kläger auch Spam auf z.B. verivox-adamriese, check24-otelo oder check24-telekom erhalten, also zufällig generierten Kombinationen. Das ist nicht der Fall, und durch das Catch-All würde das auffallen.

- In den Kundeninformationen (Anlage K5 Informationen) behauptet die Verantwortliche, „Der Betreiber der Plattform von MOVEit hat uns im Mai 2023 über einen entsprechenden Vorfall auf seiner Plattform informiert“ und „Als Teil dieser Sofort-Maßnahmen haben wir unter anderem die Nutzung von MOVEit umgehend eingestellt.“ Wie es dann möglich ist, dass eine Emailadresse betroffen ist, die erst am 23.08.2023 verwendet wurde, ist dem Kläger ein Rätsel (Anlage K6 Update vs. Bescheid Anlage 1, 2.1 f).

Die Aussagen der Verantwortlichen halten daher insgesamt einer Überprüfung nicht stand. Das beweist weder ihre Schuld noch ihre Unschuld, sondern lediglich die Mängel der forensischen Untersuchung und der Untersuchung durch den Beklagten. Auf die Beweispflicht der Verantwortlichen wurde schon hingewiesen.

In Anbetracht der schwerwiegenden Untersuchungsmängel des Beklagten erscheint die Feststellung der Nichtigkeit des Bescheids angemessen (vgl. Ramsauer in Kopp/Ramsauer, Verwaltungsverfahrensgesetz, 25. Auflage 2024, §44 Rn. 8ff), zumindest erscheint eine Heilung der Verfahrensfehler nach §§45f LVwVfG ausgeschlossen.

Mit freundlichen Grüßen



Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Baden-Württemberg | Postfach 10 29 32 | 70025 Stuttgart

Herrn
Joachim Lindenberg
Heubergstraße 1a
76228 Karlsruhe

Name: [redacted]

Telefon: +49 711 615541-[redacted]
E-Mail: poststelle@lfdi.bwl.de

Geschäftszeichen: LfDIAbt4-0554.1-124/102
(bei Antwort bitte angeben)

Datum: 6. Dezember 2024

Ihre E-Mail-Beschwerde gegen Verivox vom 28. Juli 2023; Abschluss-Schreiben
Anlagen: 2

Sehr geehrter Herr Lindenberg,

wir haben die inzwischen vorliegenden Stellungnahmen von Verivox ausgewertet.

Wir sind zum Ergebnis gekommen, dass keine Anhaltspunkte für Ihre Vermutung vorliegen, dass Ihre beiden E-Mail-Adressen verivox-telekom@lindenberg.one und verivoxotelo-vodafone@lindenberg.one durch oder bei Verivox kompromittiert worden sind. Auch ein Verkauf dieser E-Mail-Adressen an Dritte wurde verneint.

Dies hat Verivox aus unserer Sicht ausführlich, nachvollziehbar und glaubhaft dargelegt.

Um Wiederholungen zu vermeiden, verweisen wir auf die weiteren Ausführungen in den beiden Verivox-Stellungnahmen vom 28. November 2024 und 5. Dezember 2024. Diese sind diesem Schreiben als Anlagen beigefügt.

Weitergehende, überprüfbare Nachweise für Ihre Vermutung haben Sie nicht vorgelegt.

Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

Das Verfahren wird hiermit abgeschlossen.

Auf Ihre Rechte nach Art. 78 DS-GVO wird hingewiesen.

Mit freundlichen Grüßen
Im Auftrag

Anlage 1

Verivox

Verivox GmbH • Max-Jarecki-Straße 21 • 69115 Heidelberg

Der Landesbeauftragte für den Datenschutz und
Informationssicherheit Baden-Württemberg
[redacted]
Postfach 102932
70025 Stuttgart

Heidelberg, den 28. November 2024

vorab per E-Mail: poststelle@lfdi.bwl.de

Stellungnahme zur Beschwerde von Herrn Joachim Lindenberg
Geschäftszeichen: LfDIAbt4-0554.1-124/102
Ihr Schreiben vom: 07. November 2024

Sehr geehrter [redacted],

vielen Dank für Ihr Schreiben vom 07.11.2024, eingegangen bei uns am 11.11.2024, auf das wir, die Verivox GmbH (im Folgenden auch: „Verivox"), gerne wie folgt Stellung nehmen:

1. Sachverhalt

Der von dem Beschwerdeführer dargestellte Sachverhalt ist unzutreffend und stellt sich wie folgt dar:

Die beiden gegenständlichen E-Mail-Adressen

- [redacted]@lindenberg.one
- [redacted]@lindenberg.one

haben wir unter anderem im Rahmen der Erfüllung unserer unternehmerischen Tätigkeit zur Vermittlung von Telekommunikationsverträgen (hier: DSL & Mobilfunk) von dem Beschwerdeführer erhalten.

Eine Weitergabe der beiden E-Mail-Adressen an Dritte, die nicht für die Erfüllung vertraglicher Pflichten an die unten angegebenen Anbieter diente, ist nicht erfolgt. Insbesondere wurden diese E-Mail-Adressen nicht an Dritte für Werbezwecke weitergegeben, sodass ein Abgriff dieser E-Mail-Adressen in dem Zusammenhang – entgegen den Ausführungen des Beschwerdeführers – vorliegend auszuschließen ist.

Zudem möchten wir der Vollständigkeit halber anmerken, dass wir auf Anfrage des Beschwerdeführers vom 26.07.2023, ihn bereits darüber informierten, dass die gegenständliche E-Mail-Adresse ([redacted]

[redacted]@lindenberg.one) nicht Gegenstand eines Hacker- oder sonstigen Schadangriffs, insbesondere nicht des Move-IT Vorfalls, gewesen ist.

Zusammenfassend gibt es aus unserer Sicht keine Anhaltspunkte, die eine Offenlegung der gegenständlichen E-Mail-Adressen an unbefugte Dritte im Zusammenhang mit Verivox erklären.

2. Betroffene Daten

2.1 Welche Daten haben Sie über die beschwerdeführende Person seit wann gespeichert?

Folgende Daten(kategorien) haben wir aktuell über die in Ihrem Schreiben genannte beschwerdeführende Person unter folgenden E-Mail-Adressen gespeichert:

a) **Mit einer abweichenden Anschrift seit dem 25.07.2019 im Zusammenhang mit der E-Mail-Adresse: [redacted]@lindenberg.one:**
- Name, Vorname
- Geschlecht
- Geburtsdatum
- Anrede
- Postanschrift
- Telefon
- Bankdaten
- Tarifdaten und Auftragsdaten, wie Laufzeit und Kündigungsfrist
- E-Mail Opt-Out vom 03.11.2019

b) **Seit dem 08.10.2020 im Zusammenhang mit der E-Mail-Adresse: [redacted]@lindenberg.one:**
- Name, Vorname
- Geschlecht
- Geburtsdatum
- Anrede
- Postanschrift
- Telefon
- Bankdaten
- Tarif und Auftragsdaten, wie Laufzeit und Kündigungsfrist
- E-Mail Opt-Out vom 25.02.2021
- Daten in Zusammenhang mit Service-Anfragen seit dem 26.07.2023/ 09.08.2023:
  - Kundenvorgang 07959543 - 26.07.2023 (Beschwerde des Kunden in Bezug auf Erhalt von Spammails mit Bezugnahme zu Move-IT)
  - Kundenvorgang 08002876 - 09.08.2023 (Beschwerde in Bezug auf den Erhalt von Spammails mit Bezugnahme zu Move-IT)
  - Schreiben von Verivox betreffend die Information des Beschwerdeführers über den Datenleak Move-IT

c) Seit dem 28. sowie dem 29.10.2020 im Zusammenhang mit der E-Mail-Adresse: [redacted]@lindenberg.one:

- Name, Vorname
- Geschlecht
- Geburtsdatum
- Anrede
- Postanschrift
- Telefon
- Bankdaten
- Tarifdaten und Auftragsdaten, wie Laufzeit und Kündigungsfrist
- E-Mail Opt-Out vom 19.05.2021
- Daten in Zusammenhang mit Service-Anfragen seit dem 08.12.2022:
    - Kundenvorgang 07214000 vom 08.12.2022 (Betroffenenanfrage vom 08.12.2022, Antwortschreiben vom 09.12.2022 sowie dazugehörige Kommunikation).

d) Seit dem 29.10.2020 im Zusammenhang mit der E-Mail-Adresse: [redacted]@lindenberg.one:

- Name, Vorname
- Geschlecht
- Geburtsdatum
- Anrede
- Postanschrift
- Bankdaten
- Auftragsdaten
- E-Mail Opt-Out vom 30.12.2020
- Dokumente: Das Bestätigungsschreiben vom 29.10.2020 sowie die darin enthaltenen Datensätze.

e) Seit dem 15.11.2020 im Zusammenhang mit der E-Mail-Adresse: [redacted]@lindenberg.one:

- Name, Vorname
- Geschlecht
- Geburtsdatum
- Anrede
- Postanschrift
- Telefon
- Bankdaten
- E-Mail Opt-Out vom 27.01.2021
- Familienstand
- Beruf
- Jahreskosten netto
- Vertrags- sowie Tarifdaten, wie Vertragsnummer, Produkttyp, Erstelldatum, Provider, Tarif, Versicherungsschein-Nr., Versicherungsschutz Startdatum, Interessentennummer
- Auftragsdaten, wie u.a. Versicherungssumme, Vermögensschaden, Laufzeit, Selbstbeteiligung

- Dokumente: Der Antrag vom 15.11.2020 sowie die darin enthaltenen Datensätze.

f) Seit dem 28.08.2023 im Zusammenhang mit der E-Mail-Adresse: Joachim.lindenberg@[redacted]
- Name, Vorname
- Geschlecht
- Geburtsdatum
- Anrede
- Postanschrift
- Telefon
- Bankdaten
- E-Mail Opt-Out vom 15.07.2024
- Vertrags- sowie Tarifdaten, Interessentennummer
- Daten in Zusammenhang mit Service-Anfragen seit dem 05.09.2023:
  - 08104035 vom 05.09.2023, 09060193 vom 16.04.2024, Auskunftsanfrage

g) Move-IT bezogene Daten: In Bezug auf die Move-IT-bezogenen Informationen finden Sie nähere Ausführungen unter Ziffer **3.3**.

h) Weitere Schreiben:
- Das vorliegende Schreiben betreffend die aktuelle Beschwerde seit dem 11.11.2024 sowie
- eine aktuelle Auskunftsanfrage vom 05.11.2024 unter der E-Mail-Adresse [redacted]@lindenberg.one seit dem genannten Datum.

Hinweis der Vollständigkeit halber: Wir haben vorliegend die Datensätze aufgelistet, die zugehörig zu den Angaben der beschwerdeführenden Person sind sowie zu den E-Mail-Adressen, die Sie in Ihrem Schreiben vom 07.11.2024 angegeben haben. Wir haben zu dem Namen der betroffenen Person aber auch eine abweichende Adresse mit dazugehörigen Datensätzen bei uns gespeichert.

2.2 Wie verarbeiten Sie diese Daten bzw. wie haben Sie diese Daten verarbeitet?

Die Datenverarbeitung hängt von der jeweiligen Produktkategorie ab. Sobald der Auftrag über die Verivox.de abgeschlossen wird, werden die (Auftrags-)Daten in den Backendsystemen der jeweiligen Produkte gespeichert, die aus einer Datenbank und Frontendapplikationen bestehen. Die für das Produkt geschulten Mitarbeiter:innen führen die jeweilige produktbezogene Bearbeitung durch, bevor die Auftragsdaten je nach Anbieter für den sich der Kunde beim Abschluss entschieden hat, dann entweder über eine API, die der Anbieter für die Auftragsübermittlung zur Verfügung stellt, übertragen oder dateibasiert auf einem SFTP-Server abgelegt wird. Mit einem IP-Whitelisting und einer Nutzernamen-Passwort-Authentifikation wird gewährleistet, dass die Auftragsbearbeitung nur durch die beteiligten, zuständigen Rollen erfolgt.

Die Daten werden auch für die Nutzung durch den Kundenservice und u. a. E-Mailkampagnen gespeichert. Dabei haben aber entsprechend eines rollenbasierten Berechtigungskonzepts nach dem Need-to-know Prinzip nur die berechtigten Rollen Zugriff auf die Daten und verarbeiten die Daten entsprechend der vordefinierten Zwecke.

2.3 Nach welchen Rechtsgrundlagen haben Sie diese Daten verarbeitet bzw. erhoben oder anderweitig verwendet oder liegt Ihnen hierzu jeweils die Einwilligung durch die beschwerdeführende Person vor (bitte Nachweise vorlegen)?

Erfüllung des Vertrages: Die Daten des Beschwerdeführers unter Ziffer 2.1. a) bis f) (mit Ausnahme des E-Mail Opt-Outs und der Daten im Zusammenhang mit den Service- und Betroffenenanfragen) haben wir auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO zur Erfüllung des Vertrages (Erbringung der Vermittlungsleistung) erhoben und verarbeitet.

Rechtliche Verpflichtung: Die weitere Speicherung dieser Daten erfolgt auf Grundlage von Art. 6 Abs. 1 lit. c DSGVO i. V. m. den steuerrechtlichen und handelsrechtlichen Aufbewahrungsfristen (§ 147 Abs. 1 Nr. 2, 3, 4, 5, Abs. 3 Abgabenordnung (AO), § 257 Abs. 1 Nr. 2, 3, 4, Abs. 4 des Handelsgesetzbuches (HGB)).

Berechtigtes Interesse: Des Weiteren haben wir die Daten des Beschwerdeführers (E-Mail-Adresse, Name, Vorname, ggf. Auftragsdaten) im Falle von Bestandskundenwerbung auf Art. 6 Abs. 1 lit. f DSGVO i. V. m. § 7 Abs. 3 UWG gestützt.

Rechtliche Verpflichtung: Die Daten im Zusammenhang mit den Service- und Betroffenenanfragen des Beschwerdeführers unter Ziffer 2.1. b) und c) sowie die Kommunikation mit Ihnen, zur Beantwortung Ihrer Fragen aus dem gegenständlichen Schreiben vom 07.11.2024 unter 2.1 h) verarbeiten und speichern wir zur Erfüllung gesetzlicher Verpflichtungen auf Grundlage von Art. 6 Abs. 1 lit. c DSGVO. Davon umfasst ist auch die Bearbeitung der aktuellen Betroffenenanfrage vom 05.11.2024 unter Ziffer 2.1 h).

Berechtigtes Interesse: Des Weiteren verarbeiten wir die Daten im Zusammenhang mit den Service- und Betroffenenanfragen des Beschwerdeführers sowie die Kommunikation mit Ihnen unter Ziffer 2.1. b), c) und h) aufgrund berechtigten Interesses gem. Art. 6 Abs. 1 lit. f DSGVO zur Geltendmachung und Verteidigung von Rechtsansprüchen sowie zu Nachweis- und Dokumentationszwecken in Bezug auf die datenschutzkonforme Bearbeitung der Betroffenenanfragen sowie die Beantwortung der weitergehenden Fragen.

2.4 Woher stammen diese Daten

Die unter Ziffer 2.1 genannten Daten – ausgenommen das gegenständliche Behördenschreiben unter Ziffer 2.1 h) – stammen vom Beschwerdeführer selbst.

2.5 Zu welchen Zwecken wurden diese Daten erhoben und anschließend verarbeitet?

Zwecks Erfüllung des Vertrages – Zwecks Erbringung der Vermittlungsleistung: Die Daten des Beschwerdeführers unter Ziffer 2.1. a) bis f) (mit Ausnahme des E-Mail Opt-Outs und der Daten im Zusammenhang mit den Service- und Betroffenenanfragen) haben wir im Rahmen der verschiedenen Abschlüsse unter den aufgelisteten E-Mail-Adressen zur Erfüllung des Vertrages – Erbringung der Vermittlungsleistung – mit dem Beschwerdeführer verarbeitet.

Zwecks Erfüllung rechtlicher Verpflichtung - Nachweiszwecke: Weiterhin verarbeiten wir diese Daten zwecks Erfüllung gesetzlicher (steuerrechtlicher und handelsrechtlicher) Aufbewahrungspflichten sowie zwecks Nachweises zur Erbringung der Vermittlungsleistung.

Zwecks Zusendung von Werbung – Zwecks Umsetzung des Widerspruchs: Zudem haben wir die Daten des Beschwerdeführers unter Ziffer 2.1 a) bis f), insbesondere die genannten E-Mail-Adressen jeweils bis zum Widerspruch für eigene Werbezwecke verarbeitet.

Zwecks Bearbeitung von (Betroffenen)Anfragen – Zwecks Geltendmachung und Verteidigung von Rechtsansprüchen – Nachweiszwecke: Die Daten des Beschwerdeführers unter Ziffer 2.1 b) und c) im Zusammenhang mit den Serviceanfragen haben wir zum Zwecke der Bearbeitung der damaligen Betroffenenanfragen verarbeitet. Wir verarbeiten diese Daten weiterhin zu Dokumentations- und Nachweiszwecken in Bezug auf die datenschutzkonforme und fristgerechte Bearbeitung der Betroffenenanfragen sowie der Beantwortung der Fragen. Zudem verarbeiten wir diese Daten zur Geltendmachung und Verteidigung von Rechtsansprüchen.

Zwecks Bearbeitung von (Betroffenen)Anfragen – Zwecks Geltendmachung und Verteidigung von Rechtsansprüchen – Zwecks Kommunikation mit der Behörde: Die zwei aktuellen Schreiben und die dazugehörigen Daten des Beschwerdeführers unter Ziffer 2.1 h) verarbeiten und speichern wir zur datenschutzkonformen und fristgerechten Bearbeitung der aktuellen Betroffenenanfrage und aufgrund der aktuellen Beschwerde bei Ihnen sowie ggf. zur Geltendmachung und Verteidigung von Rechtsansprüchen und zwecks Kommunikation mit Ihnen (der zuständigen Datenschutzaufsichtsbehörde).

2.6 Werden/ wurden diese Daten an Dritte weitergegeben? Wenn ja, an wen, mit welcher Rechtsgrundlage und mit der Bindung an welche Zwecke?

Die unter Ziffer 2.1 a) bis f) genannten Daten des Beschwerdeführers (mit Ausnahme des E-Mail Opt-Outs und der Daten im Zusammenhang mit den Service- und Betroffenenanfragen), insbesondere die gegenständlichen zwei E-Mail-Adressen, wurden zur Erbringung unserer jeweiligen Vermittlungsleistungen gem. Art 6 Abs. 1 lit. b DSGVO an folgende Dritte weitergegeben:

Hinweis: Bei Abschluss von Telekommunikationsverträgen haben wir die Daten an den jeweiligen (unten konkretisierten) Vertragspartner übermittelt, welcher die Daten an den jeweiligen Anbieter weitergegeben hat.

a)
b)
c)
d)
e)
f)

[redacted]

Die weiteren Daten, insbesondere unter Ziffer 2.1 h) zum aktuellen Auskunftsersuchen sowie zur gegenständlichen Beschwerde wurden an keine Dritten weitergegeben mit Ausnahme unserer externen Datenschutzbeauftragten (Frau Jacqueline Neiazy, ISiCO GmbH, Am Hamburger Bahnhof 4, Berlin) und die mit der Bearbeitung des vorliegenden Sachverhalts beauftragten Personen, die bei der ISiCO GmbH angestellt sind sowie Ihnen als zuständige Datenschutzaufsichtsbehörde.

Eine Weitergabe von E-Mail-Adressen an Dritte zu Werbezwecken ist nicht erfolgt.

3. Weitergaben der E-Mail-Adressen

a) Wie kann es sein, dass der Beschwerdeführer Spammails von Dritten an die E-Mail-Adressen bekommt, die nur Ihnen im Zusammenhang mit der Nutzung Ihrer Vergleichsplattform bekannt geworden sind?

Es sind für uns keine Anhaltspunkte ersichtlich, dass der Beschwerdeführer Spam-Mails im Zusammenhang mit der Nutzung unserer Plattform erhalten hat. Insbesondere aus folgenden Gründen:

- Die gegenständlichen zwei E-Mail-Adressen sind vom Move-IT-Fall nicht betroffen, da diese Daten in Move-IT nicht enthalten sind.
- Auch bei dem CCC-Vorgang sind die beiden E-Mail-Adressen nicht betroffen gewesen (siehe hierzu auch weiter unten unter Ziffer 3. d)).
- Eine Übermittlung von E-Mail-Adressen an Dritte für Werbezwecke findet durch Verivox nicht statt. Für Werbezwecke werden die E-Mail-Adressen nur für eigene Werbezwecke bzw. für den Verivox-Newsletter der Verivox-Gruppe verwendet. Dies gilt auch für die gegenständlichen zwei E-Mail-Adressen. Diese wurden auch nur an die oben unter Ziffer 2.6 angegebenen Dritten zur Vermittlung und Vertragsdurchführung übermittelt. Eine darüberhinausgehende Übermittlung an weitere Dritte, insbesondere für Werbezwecke, ist nicht erfolgt.
- Wie die Dritten (Anbieter) selbst mit den Daten/ E-Mail-Adressen umgehen, kann der jeweiligen Webseite/ Datenschutzerklärung entnommen werden. Der Datenschutzerklärung des Anbieters Vodafone ist beispielsweise unter Ziffer 12 c zu entnehmen, dass dieser auch E-Mail-Adressen für eigene Produkte zu Werbezwecken verarbeitet. Weiterhin ist beispielsweise der Datenschutzerklärung der Telekom unter Ziffer 8 zu entnehmen, dass auch sie Daten von Kunden an Auftragsverarbeiter und Kooperationspartner übermitteln.

Wie oben ausgeführt, wäre es also auch zur weiteren Sachverhaltsaufklärung ggf. zweckmäßig zu überprüfen, ob und wie die E-Mail-Adressen von den Dritten (Anbietern) weiterverarbeitet wurden. Gegebenenfalls wäre es zum Schutz der Belange des Beschwerdeführers auch zweckmäßig, dass überprüft wird, ob er ggf. selbst die E-Mail-Adressen anderweitig verwendet hat oder ob die gegenständlichen E-Mail-Adressen ggf. über die Vielzahl der anderen genutzten E-Mail Zugänge offengelegt wurden. Aufgrund der überdurchschnittlich hohen Anzahl von verwendeten E-Mail-Adressen kann nicht ausgeschlossen werden, dass ein Abgriff an anderer Stelle erfolgte.

Verivox GmbH • Max-Jarecki-Straße 21 • 69115 Heidelberg
Postanschrift: Verivox GmbH • 69110 Heidelberg
info@verivox.de • www.verivox.de
t +49 6221 7961-0 • f +49 6221 7961-184

Registergericht Mannheim • HRB 336125 • USt-IdNr.: DE 197 999 416
Bankverbindung: Commerzbank Heidelberg
IBAN DE53 6724 0039 0196 6811 00 • SWIFT COBADEFFXXX
Geschäftsführer: Daniel Puschmann (Sprecher) • Sandra Vollmer

b) Haben Sie die beiden E-Mail-Adressen an Dritte verkauft oder vermietet?

Ein Verkauf oder eine Vermietung von E-Mail-Adressen findet durch Verivox nicht statt und wir haben die beiden E-Mail-Adressen daher auch nicht an Dritte verkauft oder vermietet.

c) Der Beschwerdeführer war von der Datenpanne Move-IT betroffen (unser Az.: LfDIAbt5-0554.1-91/95) und wurde von Ihnen am 06. August 2023 durch die Datenschutz Agentur postalisch darüber informiert. Im geleakten Datensatz ging es um diese darin enthaltene E-Mail-Adresse: [redacted]@lindenberg.one.

Können Sie damit ausschließen, dass die beiden oben genannten E-Mail-Adressen des Betroffenen auch geleakt wurden?

Nach mehrfacher Prüfung kann ausgeschlossen werden, dass die oben genannten E-Mail-Adressen im Zusammenhang mit Move-IT geleakt wurden. Diese zwei E-Mail-Adressen waren nicht in Move-IT gespeichert. Wie von Ihnen bereits ausgeführt, ging es im Move-IT-Fall um die E-Mail-Adresse [redacted]@lindenberg.one.

d) Könnte ein anderes Datenleak die Ursache sein?

Es bestehen keine Anhaltspunkte für einen Zusammenhang zwischen dem Erhalt von Spam-Mails und sonstigen Vorfällen bei Verivox und nach unserer Prüfung gab es keine weiteren Leaks, bei denen die gegenständlichen zwei E-Mail-Adressen geleakt wurden.

Dies betrifft auch insbesondere den CCC-Vorgang: Bei dem CCC-Vorgang konnten ausschließlich Verträge von Banking-Kunden eingesehen werden. Die genannten E-Mail-Adressen oder weitere Daten des Beschwerdeführers sind davon nicht betroffen, zumal der Beschwerdeführer auch kein Banking-Kunde ist, sodass auch der Vorgang mit CCC von uns als Ursache ausgeschlossen werden kann.

4. Datenlöschkonzeption

4.1 Wann und auf welche Art und Weise beabsichtigen Sie, die bei Ihnen über die beschwerdeführende Person gespeicherten Daten zu löschen?

Die Daten des Beschwerdeführers unter Ziffer 2.1 a) bis f) (mit Ausnahme des E-Mail Opt-Outs und der Daten im Zusammenhang mit den Service- und Betroffenenanfragen) löschen wir nach Ablauf der gesetzlichen Aufbewahrungspflichten nach sechs Jahren ab Beendigung des Vertrages bei Verträgen und Aufträgen sowie nach zehn Jahren bei Zahlungs- und Rechnungsdaten, im Übrigen mit dem Schluss des Kalenderjahres, in dem der Handelsbrief empfangen oder abgesandt worden und der Buchungsbeleg sowie die sonstigen Unterlagen entstanden sind.

Die unter Ziffer 2.1 h) genannten Daten des Beschwerdeführers zum hiesigen behördlichen Verfahren löschen wir nach sechs Jahren ab dem 31.12.2024 (doppelte der gesetzlichen Verjährungsfrist, s. Art. 6 Abs. 1 lit. f DSGVO i. V. m. § 33 Abs. 3 S. 2 OWIG).

Die Daten des Beschwerdeführers zu den E-Mail Opt-Outs und der Daten im Zusammenhang mit den Service- und Betroffenenanfragen sowie zu dem aktuellen Auskunftsersuchen unter Ziffer 2.1 a) bis f) und h) löschen wir auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO nach drei Jahren.

Die Löschung erfolgt teils manuell und teils automatisch (systemseitig).

4.2 Beim Vorliegen von handels- und/ oder steuerrechtlichen Aufbewahrungsvorschriften: Bitte nennen Sie uns die genauen gesetzlichen Grundlagen und die Dauer der Aufbewahrungsfrist (Fristbeginn, Fristende).

Die Daten des Beschwerdeführers unter Ziffer 2.1 a) bis f), die zur Erbringung der Vermittlungsleistung gespeichert wurden, werden aufgrund gesetzlicher Aufbewahrungspflichten gem. Art. 6 Abs. 1 lit. c DSGVO i. V. m. § 147 Abs. 1 Nr. 2, 3, 5, Abs. 3 AO i. V. m. § 257 Abs. 1 Nr. 2, 3, Abs. 4 HGB für Verträge und Aufträge für sechs Jahre und gem. Art. 6 Abs. 1 lit. c DSGVO i. V. m. § 147 Abs. 1 Nr. 4 AO, Abs. 3 AO, § 257 Abs. 1 Nr. 4, Abs. 4 HGB für Rechnungen (Rechnungs- und Zahlungsdaten) für zehn Jahre aufbewahrt. Beginn und Ende der Aufbewahrungsfristen ergibt sich aus § 147 AO, § 257 HGB.

Die Frist für die Vertrags- und Auftragsdaten sowie für Rechnungen (Rechnungs- und Zahlungsdaten) beginnt und endet danach in Bezug auf die vorhandenen Datensätze unter Ziffer 2.1 a) bis f) des Beschwerdeführers wie im Folgenden:

a) **Daten unter Ziffer 2.1 a) im Zusammenhang mit der E-Mail-Adresse: [redacted]@lindenberg.one:**

Vertrags-/ Auftragsdaten:
Fristbeginn mit Ablauf des 31.12.2019 und Fristende mit Ablauf des 31.12.2025.

Rechnungen:
Fristbeginn mit Ablauf des 31.12.2019 und Fristende mit Ablauf des 31.12.2029.

b) **Daten unter Ziffer 2.1 b) im Zusammenhang mit der E-Mail-Adresse: [redacted]@lindenberg.one:**

Vertrags-/ Auftragsdaten:
Fristbeginn mit Ablauf des 31.12.2020 und Fristende mit Ablauf des 31.12.2026.

Rechnungen:
Fristbeginn mit Ablauf des 31.12.2020 und Fristende mit Ablauf des 31.12.2030.

c) **Daten unter Ziffer 2.1 c) in Zusammenhang mit der E-Mail-Adresse: [redacted]@lindenberg.one:**

Vertrags-/ Auftragsdaten:
Fristbeginn mit Ablauf des 31.12.2020 und Fristende mit Ablauf des 31.12.2026.

Rechnungen:
Fristbeginn mit Ablauf des 31.12.2020 und Fristende mit Ablauf des 31.12.2030.

d) Daten unter Ziffer 2.1 d) im Zusammenhang mit der E-Mail-Adresse: [redacted]@lindenberg.one:

Vertrags-/ Auftragsdaten:
Fristbeginn mit Ablauf des 31.12.2020 und Fristende mit Ablauf des 31.12.2026.

Rechnungen:
Fristbeginn mit Ablauf des 31.12.2020 und Fristende mit Ablauf des 31.12.2030.

e) Daten unter Ziffer 2.1 e) im Zusammenhang mit der E-Mail-Adresse: [redacted]@lindenberg.one:

Vertrags-/ Auftragsdaten:
Fristbeginn mit Ablauf des 31.12.2020 und Fristende mit Ablauf des 31.12.2026.

Rechnungen:
Fristbeginn mit Ablauf des 31.12.2020 und Fristende mit Ablauf des 31.12.2030.

f) Daten unter Ziffer 2.1 f) im Zusammenhang mit der E-Mail-Adresse: Joachim.lindenberg@[redacted]

Vertrags-/ Auftragsdaten:
Fristbeginn mit Ablauf des 31.12.2023 und Fristende mit Ablauf des 31.12.2029.

Rechnungen:
Fristbeginn mit Ablauf des 31.12.2023 und Fristende mit Ablauf des 31.12.2033.

Wir hoffen, Ihre Fragen hiermit abschließend beantwortet zu haben. Bei Rückfragen können Sie jederzeit gern auf uns zukommen.

Mit freundlichen Grüßen

[redacted]

Data Protection Coordinator
m +49 (0) 174 744 [redacted]
adrian.blankenstein@verivox.com

Anlage 2

[redacted]
Rechtsanwalt
+49.69.6062 [redacted]
[redacted]@lw.com

[redacted]
Rechtsanwältin
+49.69.6062.[redacted]
[redacted]@lw.com

Die Welle
Reuterweg 20
60323 Frankfurt am Main
Tel: +49.69.6062.6000
Fax: +49.69.6062.6700
www.lw.com

LATHAM&WATKINS

Per beA

Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit Baden-Württemberg
[redacted]
Lautenschlagerstraße 20
70173 Stuttgart

Frankfurt am Main, 5. Dezember 2024
Unser Zeichen: 063768.0001 (TWY/IBR)

Ihr Zeichen: LfDIAbt4-0544.1-124/102
Ihre E-Mail vom 29. November 2024

Hier: Stellungnahme zu Ihren Rückfragen

Sehr geehrte [redacted],
sehr geehrte Damen und Herren,

1 wir nehmen Bezug auf Ihr Schreiben an die Verivox GmbH („**Verivox**“) vom 7. November 2024 sowie auf Ihre E-Mail an die Datenschutzbeauftragte von Verivox, [redacted], vom 29. November 2024.

2 Wir zeigen an, dass wir Verivox auch im Rahmen des gegenständlichen Beschwerdeverfahrens vertreten. Der guten Ordnung halber fügen wir die Ihrer Behörde bereits vorliegende Vollmacht nochmals bei als **Anlage 1**. Nachfolgend nehmen wir für Verivox zu den in Ihrer E-Mail vom 29. November 2024 aufgeworfenen Rückfragen Stellung.

I. Auskunft über die konkret verarbeiteten Daten

3 In Ihrer E-Mail vom 29. November 2024 baten Sie Verivox unter anderem um eine Mitteilung darüber, welche konkreten personenbezogenen Daten Verivox über den Beschwerdeführer – Herrn Joachim Lindenberg – verarbeitet. Eine entsprechende Übersicht stellen wir Ihnen als **Anlage 2** zur Verfügung.

4 Die bislang gegenüber Ihrer Behörde kommunizierten Bezeichnungen wie „Daten(kategorien)" sollten primär eine übersichtliche und strukturierte Form der Darstellung sicherstellen. Die Zusammenfassung von Daten in Datenkategorien sollte die Darstellung für Ihre Behörde noch nachvollziehbarer gestalten. Die von Verivox gewählten Begrifflichkeiten dienten hingegen keineswegs dazu, Ihrer Behörde Informationen über die konkret verarbeiteten Daten vorzuenthalten. Dementsprechend stellen wir Ihnen auch gerne eine entsprechende Datenaufstellung zur Verfügung.

5 Der Vollständigkeit halber weisen wir darauf hin, dass Verivox Antragstellern im Rahmen von Auskunftsverfahren auch die konkret verarbeiteten Daten mitteilt.

II. Kein Abhandenkommen der beiden genannten E-Mail-Adressen

6 Zum anderen baten Sie um nähere Informationen über die von Verivox durchgeführten Prüfmaßnahmen in Bezug auf die E-Mail-Adressen [redacted]@lindenberg.one und [redacted]@lindenberg.one.

7 Verivox hat hierzu die über Herrn Lindenberg gespeicherten personenbezogenen Daten nochmals eingehend im Hinblick auf die Möglichkeit einer unbefugten Offenlegung (*Leak*) geprüft.[1] Diese Prüfung umfasste gerade auch die beiden genannten E-Mail-Adressen. Nach Abschluss dieser Überprüfung kann Verivox weiterhin belastbar ausschließen, dass die beiden E-Mail-Adressen widerrechtlich von den Systemen von Verivox abgeflossen sind (insbesondere nicht im Rahmen des MOVEit-Vorfalls).

1. MOVEit-Vorfall

8 Nach Bekanntwerden des MOVEit-Vorfalls hat Verivox den betroffenen Server unmittelbar vom Netz genommen. Aktuellen IT-Sicherheitsstandards folgend, hat Verivox sodann eine forensische Kopie des vom Netz genommenen Servers angefertigt, der über keine Verbindungen zum Internet verfügte (*Quarantäne*). Diese Kopie bildet die Daten dabei in der Form ab, wie sie auch auf dem betroffenen MOVEit-Server gespeichert waren. Verivox hat diese forensische Kopie für alle weiteren Datenanalysen und insbesondere auch zur Identifizierung betroffener Kundenkontakte genutzt.

9 Anlässlich der Beschwerde von Herrn Lindenberg hat Verivox nochmals manuell überprüft, ob die genannten E-Mail-Adressen in der forensischen Kopie des MOVEit-Servers vorhanden waren. Dies war nicht der Fall. Damit kann Verivox belastbar ausschließen, dass die E-Mail-Adressen von dem MOVEit-Vorfall betroffen waren.

10 In diesem Zusammenhang weisen wir darauf hin, dass sich der MOVEit-Vorfall nicht auf andere Server von Verivox bezog. Dies galt insbesondere für die Systeme zur Verwaltung von Kundendaten. Verivox hat den MOVEit-Server gerade nicht zur Speicherung entsprechender

---

[1] Vgl. hierzu bereits die Stellungnahme von Verivox vom 28. November 2024.

Kundendaten genutzt. Vielmehr diente die MOVEit-Software ausschließlich dazu, Kundendaten zu übertragen. Daher waren auf dem MOVEit-Server regelmäßig auch keine vollständigen Kundendatensätze gespeichert.

2. CCC-Vorgang

11 Verivox hat anlässlich der Beschwerde zudem geprüft, ob die genannten E-Mail-Adressen im Rahmen des kürzlich bekannt gewordenen CCC-Vorgangs einsehbar waren. Dies war ebenfalls nicht der Fall. Eine Offenlegung der E-Mail-Adressen auf diesem Weg wäre auch fernliegend. Wie bereits in unserer Stellungnahme vom 28. November 2024 dargelegt, betraf der CCC-Vorgang ausschließlich bestimmte Daten von Kunden im Bereich Banking. Diese Daten wurden organisatorisch getrennt von anderen Kundendaten gespeichert. Es bestehen keine Möglichkeiten, über Schnittstellen auf Daten anderer Geschäftsbereiche zuzugreifen. Herr Lindenberg ist – auch nach seinen eigenen Angaben – gerade kein Banking-Kunde von Verivox.

3. Keine weiteren Vorfälle

12 Im Übrigen liegen Verivox auch keine Anhaltspunkte für weitere Vorfälle vor, die zu einer ungewollten Offenlegung der E-Mail-Adressen geführt haben könnten.

13 Verivox verfügt über umfassende und dem Stand der Technik entsprechende IT-Sicherheitssysteme zum Schutz von Kundendaten. Hierzu zählt etwa eine fortlaufende Überwachung aller relevanten Server durch Firewalls und die Verschlüsselung von Kundendaten im Ruhezustand. Diese Systeme dienen gerade dazu, mögliche Angriffe auf Kundendaten und entsprechende Datenabflüsse frühzeitig zu erkennen und zu verhindern. Verivox liegen dementsprechend auch keine Anhaltspunkte für mögliche Sicherheitslücken oder Schwachstellen im Rahmen des Internetangebots auf der URL www.verivox.de vor.

14 Vor diesem Hintergrund kann Verivox nur mutmaßen, auf welchem Weg die genannten E-Mail-Adressen von Herrn Lindenberg möglicherweise offengelegt worden sein könnten. Zum einen erscheint es nicht ausgeschlossen, dass die E-Mail-Adressen bereits in den Systemen von Herrn Lindenberg – etwa verursacht durch entsprechende Sicherheitslücken – widerrechtlich abgeflossen sind. Herr Lindenberg scheint offenbar eine große Zahl von E-Mail-Adressen zu nutzen. Daher ist es denkbar, dass Herr Lindenberg seine zahlreichen E-Mail-Adressen in den von ihm genutzten Mailboxen oder anderen IT-Systemen dokumentiert hat.

15 Zum anderen weisen wir darauf hin, dass Herr Lindenberg unter seinem Blog blog.lindenberg.one/Themen zahlreiche mit Behörden und Unternehmen geführte Korrespondenzen selbst offenlegt. Aufgrund dieser umfassenden publizistischen Tätigkeit halten wir es auch für möglich, dass Herr Lindenberg die genannten E-Mail-Adressen selbst im Internet offengelegt haben könnte.

16 Abschließend weisen wir darauf hin, dass Verivox in der Vergangenheit bereits mehrfach Kundenbeschwerden zu ähnlichen Sachverhalten erhalten hat. Auch in diesen Fällen haben die da-

LATHAM&WATKINS LLP

raufhin eingeleiteten Untersuchungen jeweils keine Anhaltspunkte für eine mögliche Offenlegung von E-Mail-Adressen durch Verivox ergeben. Insbesondere hat Verivox bereits lange vor dem MOVEit-Vorfall immer wieder Beschwerden über Spam-Nachrichten an E-Mail-Adressen erhalten, welche nach Aussagen von Kunden speziell für die Kommunikation mit Verivox eingerichtet wurden. Auch in diesen Fällen konnte Verivox als mögliche Ursache für die Zusendung dieser unverlangten E-Mails keine Schwachstelle auf ihren Systemen feststellen.

17 In diesem Zusammenhang ist ebenfalls zu bedenken, dass auch speziell für einen Nutzungszweck eingerichtete E-Mail-Adressen häufig aus sehr generischen und für Dritte leicht nachvollziehbaren Bestandteilen bestehen. Solche E-Mail-Adressen weisen oftmals eine eher simple Systematik bzw. Strukturierung auf. Es ist durchaus denkbar, dass Dritte durch das bloße Testen von Wortkombinationen entsprechende E-Mail-Adressen erraten. Dies könnte auch im Hinblick auf die E-Mail-Adressen von Herrn Lindenberg der Fall gewesen sein. Denn die von ihm genutzte Systematik zur Benennung seiner Empfangsadressen ist aus den zwei genannten E-Mail-Adressen („[redacted]" und „[redacted]") ohne weiteres ableitbar.

18 Wir sind natürlich gerne dazu bereit, Ihrer Behörde bei Bedarf weitergehende Informationen in Bezug auf den gegenständlichen Vorgang bereitzustellen. Wir können uns hierzu auch gerne telefonisch abstimmen, wenn Sie dies möchten.

Mit freundlichen Grüßen

[redacted] [redacted]

Anlagen:

- Anlage 1: Vollmacht
- Anlage 2: Übersicht über die zum Beschwerdeführer verarbeiteten personenbezogenen Daten

```
Anlage 1 liegt dem Kläger nicht vor,
Anlage 2 ist nicht relevant
```

LATHAM & WATKINS LLP

Düsseldorf
Benrather Straße 18–20
40213 Düsseldorf
Tel: +49.211.8828.4600
Fax: +49.211.8828.4699

Frankfurt
Reuterweg 20
60323 Frankfurt am Main
Tel: +49.69.6062.6000
Fax: +49.69.6062.6700

Hamburg
Warburgstraße 50
20354 Hamburg
Tel: +49.40.4140.30
Fax: +49.40.4140.3130

München
Maximilianstraße 13
80539 München
Tel: +49.89.2080.3.8000
Fax: +49.89.2080.3.8080

Düsseldorf

[redacted]

Frankfurt

[redacted]

Hamburg

[redacted]

München

[redacted]

Anlage K4 Mitre

Full-Screen View

CVE-ID

CVE-2023-34362

Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:http://packetstormsecurity.com/files/172883/MOVEit-Transfer-SQL-Injection-Remote-Code-Execution.html
- MISC:http://packetstormsecurity.com/files/173110/MOVEit-SQL-Injection.html
- MISC:https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

Assigning CNA

MITRE Corporation

Date Record Created

20230602

Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20230602)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

Ausführliche Kundeninformation: Datenschutzinformation gemäß Art. 34 DSGVO (Stand: März 2024)

Liebe Nutzerinnen und Nutzer von Verivox,

wir möchten Sie im Folgenden über einen Datenvorfall im Zusammenhang mit der Datenübertragungssoftware MOVEit ("**MOVEit**") informieren, der unter anderem auch personenbezogene Daten von Kundinnen und Kunden von Verivox ("**Kunden**") betraf ("**Vorfall**").

Was ist passiert?

Uns ist der Schutz von personenbezogenen Daten unserer Kunden sehr wichtig. Daher haben wir umfassende technische und organisatorische Maßnahmen umgesetzt, um ein möglichst hohes Maß an Datensicherheit bei der Verarbeitung personenbezogener Daten zu gewährleisten. Trotz dieser umfassenden Maßnahmen lässt sich das Risiko möglicher Datenvorfälle nicht immer vollständig ausschließen. Der Betreiber der Plattform von MOVEit hat uns im Mai 2023 über einen entsprechenden Vorfall auf seiner Plattform informiert.

Bei MOVEit handelt es sich um eine verschlüsselte Datei-Übertragungssoftware, die tausende Unternehmen und Organisationen weltweit zur möglichst sicheren Übertragung von Daten genutzt haben – so auch Verivox. Der Betreiber von MOVEit teilte uns mit, dass es Hackern gelungen sei, über eine Schwachstelle bei MOVEit die Verschlüsselung der Daten zu umgehen, die auf der Plattform in verschlüsselter Form gespeichert waren. Diese Schwachstelle hat es den Hackern nach Angaben des Betreibers von MOVEit ermöglicht, unter anderem auch von Verivox verarbeitete Kunden-Daten widerrechtlich abzurufen. Daneben waren tausende andere Unternehmen sowie Behörden von dem Vorfall betroffen.

haben nach Kenntniserlangung unverzüglich Maßnahmen ergriffen, um den Vorfall aufzuklären und mögliche Folgen oder Risiken für betroffene Kunden zu verringern. Als Teil dieser Sofort-Maßnahmen haben wir unter anderem die Nutzung von MOVEit umgehend eingestellt. Zudem haben wir den Server, auf dem MOVEit lief, komplett neu aufgesetzt. Es ist daher ausgeschlossen, dass sich der Vorfall in dieser oder ähnlicher Form wiederholen könnte. Vorsorglich haben wir unsere hohen Sicherheitsstandards weiter verstärkt, beispielsweise durch den Ausbau unserer Firewall.

Da uns ein hohes Maß an Transparenz sehr wichtig ist, haben wir unmittelbar nach Bekanntwerden des Vorfalls eine öffentliche Mitteilung über den Vorfall auf unserer Startseite veröffentlicht. Weiterhin haben wir die zuständigen Behörden sowie die Presse über den Vorfall informiert. Wir haben uns in Bezug auf den Vorfall insbesondere mit der für uns zuständigen Datenschutzaufsichtsbehörde abgestimmt.

Nach Abschluss unserer internen Aufklärungsmaßnahmen haben wir weiterhin die als betroffen identifizierten Kunden individuell über den Vorfall informiert.

Welche Daten sind betroffen?

Auf der Basis der uns vorliegenden Prüfergebnisse waren vor allem folgende personenbezogene Daten von Kunden von dem Vorfall betroffen: Name, Anschrift, Geburtsdatum, E-Mail-Adresse, Telefonnummer und Vertragsdaten. In bestimmten Fällen waren auch Bankverbindungsdaten betroffen (Kreditinstitut, IBAN).

Wir haben die betroffenen Kunden jeweils individuell über die bei ihnen betroffenen Daten informiert.

Welche Folgen hat der Vorfall?

Uns liegen bis jetzt keine Anhaltspunkte dafür vor, dass die von dem Vorfall betroffenen Daten missbräuchlich verwendet worden sein könnten. Uns sind auch keine sonstigen Nachteile oder Risiken für die vom Vorfall betroffenen Kunden bekannt. Entsprechende Risiken (wie z.B. ein Identitätsdiebstahl) lassen sich aber zum jetzigen Zeitpunkt nicht vollständig ausschließen.

Sie haben weitere Fragen?

Wir sind für Sie da. Sollten Sie weitere Fragen haben, können Sie sich jederzeit mit einer E-Mail an *sicherheit@verivox.de* wenden.

Joachim Lindenberg

Von: Verivox Datenschutzinformation <no-reply@verivox.de>
Gesendet: Freitag, 22. Dezember 2023 11:18
An: joachim.lindenberg@[redacted]
Betreff: Update in Bezug auf den Schutz Ihrer personenbezogenen Daten

Liebe(r) Joachim Lindenberg

ein hohes Maß an Transparenz gegenüber unseren Kundinnen und Kunden (nachfolgend Kunden) ist uns sehr wichtig. Daher hatten wir unsere Kunden bereits am 16. Juni 2023 auf unserer Homepage über einen Vorfall im Zusammenhang mit der MOVEit-Plattform informiert. Seitdem haben wir die Ursachen und möglichen Auswirkungen des Vorfalls weiter intensiv aufgearbeitet. Hierzu möchten wir Ihnen gerne nachstehend ein Update geben und Ihnen näher erläutern, inwiefern Ihre personenbezogenen Daten von dem Vorfall betroffen waren.

Auch mehr als sechs Monate nach Bekanntwerden des Vorfalls liegen uns keine Anhaltspunkte dafür vor, dass die von dem Vorfall betroffenen Daten missbräuchlich verwendet worden sein könnten. Uns sind nach wie vor auch keine sonstigen Nachteile oder Risiken für die vom Vorfall betroffenen Kunden bekannt.

Soweit Sie im Einzelfall ein Vertragsverhältnis mit der Verivox Versicherungsvergleich GmbH und / oder der Verivox Finanzvergleich GmbH als Vertragspartnerin abgeschlossen haben, beziehen sich die Inhalte der vorliegenden Mitteilung gleichermaßen auch auf die Verivox Versicherungsvergleich GmbH beziehungsweise die Verivox Finanzvergleich GmbH.

Was ist passiert?

Uns ist der Schutz der personenbezogenen Daten unserer Kunden sehr wichtig. Daher haben wir umfassende technische und organisatorische Maßnahmen umgesetzt, um ein möglichst hohes Maß an Datensicherheit bei der Verarbeitung von personenbezogenen Daten zu gewährleisten. Trotz dieser umfassenden Maßnahmen lässt sich das Risiko von möglichen Datenvorfällen nicht immer vollständig ausschließen. Der Betreiber der Plattform von MOVEit, die von uns zum gesicherten Teilen von Daten genutzt wurde, hat uns am 31. Mai 2023 über einen entsprechenden Vorfall auf seiner Plattform informiert.

Bei MOVEit handelt es sich um eine verschlüsselte Datei-Übertragungssoftware, die tausende Unternehmen und Organisationen weltweit zur möglichst sicheren Übertragung von Daten genutzt haben – so auch Verivox. Der Betreiber von MOVEit teilte uns mit, dass es Hackern gelungen sei, über eine Schwachstelle bei MOVEit die Verschlüsselung der Daten zu umgehen, die auf der Plattform in verschlüsselter Form gespeichert waren. Diese Schwachstelle hat es den Hackern nach Angaben des Betreibers von MOVEit ermöglicht, auch von Verivox verarbeitete Daten widerrechtlich abzurufen. Somit waren auch Daten von Verivox-Kunden von diesem Vorfall betroffen.
Die Aufklärung des Umfangs des Vorfalls sowie die Ermittlung einzelner betroffener Kunden gestaltete sich aufgrund der Speicherstrukturen der betroffenen Daten für uns als ausgesprochen herausfordernd und aufwändig.

Welche Maßnahmen haben wir getroffen?

Wir haben nach Kenntniserlangung unverzüglich Maßnahmen ergriffen, um den Vorfall aufzuklären und mögliche Folgen oder Risiken für betroffene Kunden von Verivox zu verringern. Als Teil dieser Sofort-Maßnahmen haben wir die Nutzung von MOVEit umgehend eingestellt. Zudem haben wir den Server, auf dem MOVEit lief, komplett neu aufgesetzt. Es ist daher ausgeschlossen, dass sich der Vorfall in dieser Form wiederholen könnte. Vorsorglich haben wir unsere hohen Sicherheitsstandards weiter verstärkt, beispielsweise durch den Ausbau unserer Firewall.

Da uns ein hohes Maß an Transparenz gegenüber unseren Kunden sehr wichtig ist, haben wir unmittelbar nach Bekanntwerden des Vorfalls eine öffentliche Mitteilung über den Vorfall auf unserer Startseite veröffentlicht. Zudem haben wir die zuständigen Behörden sowie die Presse über den Vorfall informiert.

Wie haben wir den Sachverhalt aufgeklärt?

In den vergangenen Monaten haben wir mit Hochdruck an der Identifizierung der von dem Vorfall betroffenen Kunden und deren jeweils betroffenen personenbezogenen Daten gearbeitet. Dies gestaltete sich als ausgesprochen herausfordernd, da wir zunächst die Datensätze mit personenbezogenen Daten herausfiltern mussten. Diese Datensätze weisen teils eine komplexe Struktur auf, da bestimmte Datensätze aus mehreren unterschiedlichen Dokumenten und anderen Dateien bestehen. Einige Datensätze beziehen sich zudem gleichzeitig auf mehrere Personen, etwa beim Abschluss von Verträgen für verschiedene Familienmitglieder.

Um den Vorgang zu beschleunigen, haben wir externe IT-Spezialisten hinzugezogen. Wegen der beschriebenen Komplexität des Vorfalls konnten wir die entsprechende Prüfung erst jetzt weitestgehend abschließen.

Welche Daten waren betroffen?

Auf der Basis der uns nun vorliegenden Prüfergebnisse waren folgende personenbezogene Daten über Sie von dem Vorfall betroffen:
Name, Anschrift, Geburtsdatum, Vertragsdaten, E-Mail-Adresse, Bankdaten, Kunden-ID.

Es kommt vor, dass Kunden auf der Verivox-Plattform auch Verträge für andere Personen abschließen (wie etwa Familienmitglieder) und/oder im Rahmen eines Vertragsabschlusses auch personenbezogene Daten Dritter eingeben. Sollte dies bei Ihnen vor Mai 2023 der Fall gewesen sein, bitten wir Sie, diese Dritten selbst über den Vorfall zu informieren oder uns deren Kontaktdaten unverzüglich zur Verfügung zu stellen. Aus den vorstehend beschriebenen technischen Gründen und aufgrund des Umstands, dass wir nur eingeschränkt Daten über diesen Personenkreis erheben, können wir diese Personen derzeit leider in solchen Fällen nicht selbst benachrichtigen.

Welche Folgen hat der Vorfall?

Uns liegen bis jetzt – mehr als sechs Monate nach Bekanntwerden des Vorfalls – keinerlei Anhaltspunkte dafür vor, dass die von dem Vorfall betroffenen Daten missbräuchlich verwendet worden sein könnten. Uns sind auch keine sonstigen Nachteile oder Risiken für die vom Vorfall betroffenen Kunden bekannt. Entsprechende Risiken (wie z.B. ein Identitätsdiebstahl) lassen sich aber zum jetzigen Zeitpunkt nicht restlos ausschließen.

Wo erhalte ich weitere Informationen?

Bei Fragen können Sie sich gerne an unseren Datenschutzbeauftragten wenden. Diesen erreichen Sie unter der folgenden Anschrift:

Maximilian Hartung
SECUWING GmbH & Co. KG | Datenschutz Agentur
Frauentorstraße 9
86152 Augsburg
E-Mail: epost@datenschutz-agentur.de

Daneben können Sie auch gerne unseren Informationssicherheitsbeauftragten Marc Rebmann via itsecurity@verivox.com kontaktieren.

Weitere Informationen zum Schutz Ihrer personenbezogenen Daten finden Sie auch in unserer Datenschutzerklärung unter https://www.verivox.de/company/datenschutz/.

Wir wünschen Ihnen – trotz dieser Neuigkeiten – frohe Weihnachten und einen guten Start ins neue Jahr.

Viele Grüße

Ihr Verivox-Team

Impressum
Verivox GmbH, Max-Jarecki-Straße 21, D-69115 Heidelberg

Telefon: +49 (0) 6221 777 00 10
Telefax: +49 (0) 6221 7961 184

Geschäftsführer: Daniel Puschmann (Sprecher), Sandra Vollmer
Eingetragen im Handelsregister beim Amtsgericht Mannheim (HRB 336125)
Sitz und Gerichtsstand der Gesellschaft ist Heidelberg
USt.-ID: DE 197999416

Inhaltlich Verantwortlicher nach §55 RStV:
Daniel Puschmann, Max-Jarecki-Straße 21, 69115 Heidelberg