Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

LfDI Baden-Württemberg · Postfach 10 29 32 · 70025 Stuttgart

Per Einschreiben gegen Rückschein:

Herrn
Joachim Lindenberg
Heubergstraße 1a
76228 Karlsruhe

Datum 15. März 2024
Name [redacted]
Durchwahl 0711/615541-[redacted]
Aktenzeichen Neu: LfDIAbt3-4400-40/9
(Alt: 0554.1-23/605)
(Bitte bei Antwort angeben)

Datenschutz im Zusammenhang mit der Übermittlung von Corona-Testergebnissen
Ihre Eingabe vom 4. Oktober 2022 und unser Schreiben vom 3. April 2023
Datenschutzaufsichtsbehördliches Verfahren

Sehr geehrter Herr Lindenberg,

dass wir Ihnen erst heute, das Ergebnis unserer datenschutzrechtlichen Prüfung mitteilen können, bitten wir zu entschuldigen. Wir haben einen Verstoß gegen die Anforderungen des technischen und organisatorischen Datenschutzes nach Artikel 25 Absatz und Artikel 32 Absatz 1 Buchstabe a der Datenschutz-Grundverordnung (folgend: DS-GVO) durch die Beschwerdegegnerin der [redacted] festgestellt und eine Verwarnung gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO gegen diese ausgesprochen.

Im Einzelnen:

I. Zum Sachverhalt

Die [redacted] (Beschwerdegegnerin), [redacted] hatte bis [redacted] in Ihrem Angebot, Tests auf das Coronavirus

SARS-CoV-2 durchzuführen. Sie haben sich als Beschwerdeführer mehrmals von der Beschwerdegegnerin auf das Coronavirus SARS-CoV-2 testen lassen. Nach den durchgeführten Tests, haben Sie von der Beschwerdegegnerin das Testergebnis in einem PDF-Dokument per E-Mail erhalten, wobei Ihr Geburtsdatum, als Passwort diente. Dieses Passwort haben Sie als Kunde separat bei der Anmeldung erfahren. Für die Verarbeitung der Testdaten setzte die Beschwerdegegnerin Cloud-Dienste des Dienstleisters „No-Q GmbH" ein. Nach den Angaben der Beschwerdegegnerin wurde das Testergebnis verschlüsselt übermittelt und für die Kunden nur über deren persönlichen E-Mail-Account zugänglich. Die Beschwerdegegnerin hat für die Kunden, die keine digitale Anmeldung vor Ort wünschten, die Mitteilung des Testergebnisses in Papierform vorgesehen.

Nach der telefonischen Kontaktaufnahme der Beschwerdegegnerin mit Ihnen, hätten Sie ihr mitgeteilt, dass Sie die Testergebnisse in Papierform nicht wollten, weil es Ihnen um das Problem der Verschlüsselung von Datenverarbeitungen als Grundsatzthematik in Deutschland ginge, und dass ein Geburtsdatum nicht als Passwort dienen dürfe.

Sie vertreten die Auffassung, dass ein Geburtsdatum leicht zu erraten oder ggf. bekannt sei und dies damit ein unzureichendes Passwort für den Schutz eines PDF-Dokuments mit dem Testergebnis sei, was per E-Mail ohne Transportverschlüsselung versandt wurde. Die Anforderungen des Artikels 32 DS-GVO seien damit nicht erfüllt. Ferner haben Sie ausgeführt, dass der von der Beschwerdegegnerin eingesetzte Dienstleister No-Q GmbH keine für den E-Mail-Versand qualifizierte Transportverschlüsselung eingesetzt habe, was Sie mit einer von Ihnen verwendeten speziellen E-Mail-Adresse haben feststellen können.

Die Beschwerdegegnerin trägt vor, dass sie in Anbetracht der hohen Sicherheitsanforderungen für die Verarbeitung der Testergebnisse über das das Coronavirus SARS-CoV-2 einen professionellen No-Q GmbH gewählt habe, dessen bereitgestellte Cloud-Dienste die Möglichkeit der Verschlüsselung vorsehe. Für die Übermittlung der Testergebnisse mit dem passwortgeschützten PDF-Dokument habe man sich wegen der Umsetzbarkeit im Alltag entschieden.

II. Rechtliche Bewertung

Es liegt ein Verstoß gegen den einzuhaltenden Stand der Technik nach Artikel 25 Absatz 1, 32 Absatz 1 Buchstabe a DS-GVO vor, da die Beschwerdegegnerin als

Verantwortliche die Testergebnisse der Corona-Tests in mit einem schwachen Passwort geschützten PDF-Dokument per E-Mail versandt hat. Darin liegt eine Verletzung des Grundsatzes der Vertraulichkeit und Integrität nach Artikel 5 Absatz 1 Buchstabe f DS-GVO.

1. Datenschutzrechtliche Verantwortlichkeit

Die Beschwerdegegnerin betreibt [redacted] und hat Tests auf das Coronavirus SARS-CoV-2 in eigener datenschutzrechtlicher Verantwortung nach Artikel 4 Nummer 7 DS-GVO angeboten. Dabei hat sie über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entschieden und den Auftragsverarbeiter „No-Q GmbH" nach Artikel 28 DS-GVO für die durchgeführten Testungen und Mitteilung der Testergebnisse Coronavirus SARS-CoV-2 eingesetzt.

2. Technische und Organisatorische Maßnahmen

a. Zu berücksichtigende Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail

Im Bereich des E-Mail-Versands und -Empfangs gibt es verschiedene Möglichkeiten der Verschlüsselung. Ohne Verschlüsselung können auch beteiligte Dienstleister oder Angreifer auf dem Transportweg über das Internet mithören oder nach Versand bzw. Empfang auf die E-Mails zugreifen und die Inhalte, die Absender und Empfänger erkennen.

Mit der Transportverschlüsselung wird die laufende Kommunikation verschlüsselt, also temporär auf dem Transportweg bzw. auf allen Zwischenschritten beim Transport, der sich über mehrere E-Mail-Server erstrecken kann. Die beteiligten E-Mail-Dienstanbieter oder erfolgreiche Angreifer auf jedem der beteiligten E-Mail-Server könnten den Inhalt einer solchen E-Mail dennoch vollständig zur Kenntnis nehmen, da nur der Transportweg geschützt ist und der Inhalt bei den E-Mail-Dienstanbietern im Klartext vorliegt. Ob eine Transportverschlüsselung zum Einsatz kommt und die Wahl des notwendigen Verschlüsselungsverfahrens, unterliegt der technischen Aushandlung zwischen den beteiligten E-Mail-Servern. Entscheidend ist die Frage, ob eine Transportverschlüsselung zustande kommt:

- Bei der *opportunistischen Transportverschlüsselung* versuchen die beteiligten E-Mail-Server (Sender und Empfänger), eine verschlüsselte Verbindung

aufzubauen. Wenn beide die Verschlüsselung unterstützen, wird auf eine verschlüsselte Verbindung gewechselt und die Übermittlung erfolgt verschlüsselt. Wenn keine Verschlüsselung zustande kommt, wird die E-Mail ohne Transportverschlüsselung zugestellt.

- Eine höhere Sicherheit bietet die *obligatorische Transportverschlüsselung*: Wenn keine Verschlüsselung zustande kommt, lehnt der E-Mail-Server, der die obligatorische Transportverschlüsselung erfordert (also Sender oder Empfänger), die weitere Übermittlung ab. Die E-Mail ist in dieser Konstellation nicht zustellbar.
- Bei der *qualifizierten Transportverschlüsselung* prüfen Sender und/oder Empfänger zusätzlich, ob es sich bei der Gegenseite tatsächlich um die richtige Gegenseite handelt. Andernfalls wird die Zustellung abgebrochen und die E-Mail ist nicht zustellbar.

Die Mehrheit der E-Mail-Dienstanbieter verwendet heutzutage eine opportunistische Transportverschlüsselung. Das bedeutet in der Praxis, dass zwar meistens eine Transportverschlüsselung zustande kommt, aber die Zustellung Vorrang vor der Sicherheit hat und im Zweifel die Transportverschlüsselung vor der Zustellbarkeit zurücktritt.

Demgegenüber verschlüsselt eine Inhalts- bzw. Ende-zu-Ende-Verschlüsselung Teile oder alle Inhalte einer E-Mail. Dies geschieht unabhängig vom Transportweg und von der Transportverschlüsselung. Der Vorteil ist, dass die so verschlüsselten Inhalte auch vor Einblicken der beteiligten E-Mail-Dienstanbieter oder erfolgreichen Angreifer auf die E-Mail-Konten geschützt sind. Solche Angriffe, z. B. mittels Phishing, kommen häufig vor. Allerdings können mit Inhalts- oder Ende-zu-Ende-Verschlüsselung nur die Inhalte der E-Mail selbst verschlüsselt werden, nicht die Metadaten insbesondere über die Sender und Empfänger. Zudem erfordert es eine technische Unterstützung durch die Sender und Empfänger und nicht nur der im Hintergrund beteiligten E-Mail-Dienstanbieter.

- Eine einfache Inhalts-Verschlüsselung kann z.B. mittels verschlüsselter PDF-Dateien erfolgen. Dann ist der Austausch der Passwörter auf einem gesicherten Kanal notwendig. Dies erfordert besondere Sicherheitsvorkehrungen bei der Auswahl und der Übermittlung der Passwörter. Sind die Passwörter nur einfach aufgebaut, können Angreifer mit Zugang zu der Datei alle Passwortvarianten automatisiert ausprobieren und so in kurzer Zeit den Zugriff auf die Daten vornehmen.

- Bei fortschrittlicheren Verfahren der Ende-zu-Ende-Verschlüsselung mittels sog. asymmetrischer Verschlüsselung (z.B. nach dem Internet-Standard RFC 4880) ist kein Austausch eines Klartext-Passworts nötig. Der Austausch der notwendigen Schlüsseldateien kann auch über einen öffentlichen und vollkommen ungesicherten Kanal erfolgen, und die nachfolgende Verschlüsselung ist trotzdem sicher. Eine solche Verschlüsselung ist die sicherste Form der Verschlüsselung.

b. Versand der Testergebnisse als PDF-Dokument mit dem Geburtsdatum als Passwort per E-Mail

Die Beschwerdegegnerin verwendete für die Übermittlung der Testergebnisse ein E-Mail-System, das die *opportunistische Transportverschlüsselung* vorsah. Für die Inhaltsverschlüsselung hat die Beschwerdegegnerin PDF-Dateien verwendet, die mit dem Geburtsdatum den der Testperson als Passwort dem Schutz des Dokuments dienten.
Es handelt sich bei den Testergebnissen über das Coronavirus SARS-CoV-2 um besondere Kategorien personenbezogener Daten – namentlich Gesundheitsdaten – nach Artikel 9 Absatz 1 und Artikel 4 Nummer 15 DS-GVO. Mit der Verarbeitung besonderer Kategorien personenbezogener Daten nach der DS-GVO geht die Vermutung einher, dass ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Daher gelten hohe Schutz- und Vertrauensanforderungen für die umzusetzenden technischen und organisatorischen Maßnahmen. Nach Artikel 32 Absatz 1 Buchstabe a DS-GVO sind die Testergebnisse über das Coronavirus SARS-CoV-2 daher wirksam verschlüsselt zu übermitteln und ein angemessener Schutz vor und nach der Übermittlung über den eigentlichen Transportweg vorzusehen. Demnach war der von der Beschwerdegegnerin eingesetzte Auftragsverarbeiter im Sinne des Artikels 28 Absatz 3 DS-GVO derart anzuweisen, dass die Übermittlung der Testergebnisse dem hohen Schutz- und Vertrauensniveau angemessen verschlüsselt zu erfolgen hat.
Die Übermittlung eines passwortgeschützten PDF-Dokumentes mit den Testergebnissen per E-Mail stellt keinen ausreichenden Schutz dar, denn ein sechsstelliges Geburtsdatum als „Passwort" ist ein unzureichender Schutz: Bei Geburtsdaten ergeben sich somit alle Tage zwischen dem 01.01.00 und dem 31.12.99 und damit 36.524 mögliche Geburtstage als Kombinationsmöglichkeiten als infrage kommende Passworte. Bei einer freien Wahl eines sechsstelligen Zahlencodes von 000000 bis 999999 wären es eine Million mögliche Passworte. Beides stellt für computergestützte Methoden kein zeitliches Hindernis dar, um einen Zugang zu erlangen, da

moderne „Passwort-Cracking-Programme“ auf handelsüblichen Computern für das Ausprobieren einer Million Passwörter nur wenige Sekunden benötigen.

c. Einzuhaltender Stand der Technik für die Übermittlung der Testergebnisse über eine E-Mail

Als verantwortliche Stelle ist die Beschwerdegegnerin gesetzlich gehalten, selbst und über den Auftragsverarbeiter, die mit der Verarbeitung der Testergebnisse verbundenen hohen Risiken hinreichend zu mindern, vgl. Artikel 24 und Artikel 25 DS-GVO. Die Beschwerdegegnerin muss hierbei Art, Umfang, Umstände und Zwecke ihrer Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen, vgl. hierzu den Erwägungsgrund 75 zur DS-GVO. Entsprechend sind infolge dieser Bewertung die technischen und organisatorischen Anforderungen für die sichere Übermittelung von Gesundheitsdaten per E-Mail festzustellen, vgl. hierzu die Orientierungshilfe der Datenschutzkonferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021, Seite 2 und 6 unter „4.2.2. Versand von E-Mail-Nachrichten bei hohem Risiko“, abrufbar unter: https://lfdi-bw.de/dsk-oh-email.

Damit die Transportverschlüsselung schützend wirken kann, haben sowohl der E-Mail-Ausgangsserver der Beschwerdegegnerin als Senderin, wie auch der E-Mail-Eingangsserver des Empfängers die ausreichenden technischen Maßnahmen durchzuführen. Dabei liegt zwar die Verantwortung für den sicheren Versand der E-Mail bei dem Sender und gleichzeitig ist der Empfänger gehalten die technischen Voraussetzungen für einen sicheren Empfang der E-Mail vorzusehen. Wenn die Beschwerdegegnerin die obligatorische oder qualifizierte Transportverschlüsselung durchgeführt hätte, wäre es nicht möglich gewesen, Ihnen das Testergebnis per E-Mail zu übermitteln. Insofern steht Ihr eigener Beitrag im Sinne eines Selbstdatenschutzes in Frage, zumal Sie die Mitteilung des Testergebnisses in Papierform nicht wünschten. Bei der Abwägung über die Zulässigkeit der durchgeführten technischen Maßnahmen ist auch zu bewerten, welche Folgen eine obligatorische (oder gar qualifizierte) Transportverschlüsselung hätte: Mit der Transportverschlüsselung wären die E-Mails mit dem Ergebnis des Corona-Tests nicht zustellbar und im besten Falle würde die Beschwerdegegnerin eine Fehlermeldung über die Unzustellbarkeit erhalten. Dies würde der Erwartungshaltung der Empfänger und der notwendigen raschen Übermittlung von Testergebnissen für ggf. notwendige Folgemaßnahmen entgegenstehen. Unberechtigte Dritte könnten, sofern der Inhalt der E-Mail ausreichend verschlüsselt

ist und keine Transportverschlüsselung zustande kommt, nur die Information erhalten, dass der Empfänger einen Corona-Test durchgeführt hat, aber nicht welches Ergebnis dieser Test hat. Die Tatsache, dass eine natürliche Person einen Corona-Schnelltest durchgeführt hat, stellt in Anbetracht der in der Pandemiezeit von der überwiegenden Mehrheit an BürgerInnen durchgeführten Corona-Tests unseres Erachtens kein hohes Risiko für die Rechte und Freiheiten im Sinne eines potentiellen Schadens nach dem Erwägungsgrund 75 zur DS-GVO dar.

Im Ergebnis wäre daher eine opportunistische Transportverschlüsselung im konkreten Fall ausreichend, wenn eine ausreichende Verschlüsselung des Inhalts durchgeführt worden wäre. Wie die Beschwerdegegnerin im Einzelnen den Stand der Technik umsetzt, kann abhängig von den Umständen des Anwendungsfalls variieren. Nach Artikel 25 Absatz 1 DS-GVO ist der Stand der Technik zu *berücksichtigen*, so dass die angewendete technische Maßnahme für einen bestimmten Anwendungsfall sich unterscheiden kann, solange das Vertrauens- und Schutzniveau gewahrt bleibt.

Schließlich haben wir die Beschwerdegegnerin darauf hingewiesen, dass die Corona-Warn-App eine Funktionalität vorsah, um die Testergebnisse auf das das Coronavirus SARS-CoV-2 in der Applikation abzurufen, womit eine sichere Übermittlung der Testergebnisse möglich und eine zusätzliche Verarbeitungen personenbezogener Daten über einen anderen Anbieter vermeidbar gewesen wäre, vgl. https://www.coronawarn.app/de/faq/results/?search=&topic=application.

Mit eventuellen Rückfragen können Sie sich über die Durchwahl [redacted] an uns wenden.

Mit freundlichen Grüßen
Im Auftrag
[redacted]