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

Joachim Lindenberg, Heubergstraße 1a, 76228 Karlsruhe

Aktenzeichen: 24.56.2025-0003298

Verwaltungsgericht Düsseldorf

Anhörung vom 27.01.2026

Telefax 0211 8891-4000

Karlsruhe, den 30.01.2026

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

vielen Dank für Ihr Schreiben vom 27.01.2026 Az. 24.56.2025-0003298. Es befremdet mich, eine Anhörung als Entwurf des Bescheids zu bekommen, das lässt mich an der Ernsthaftigkeit und Ergebnisoffenheit der Anhörung zweifeln (s.a. Kallerhoff/Mayen in Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 10. Aufl. 2022, VwVfG § 28 Rn. 38).

Auch Ihre Feststellung „Diese Stellungnahmen wurden Ihnen zur Kenntnisnahme und Äußerung übersandt." befremdet mich, ich habe mit Email vom 23.10.2025 (S. 206 der ans Gericht übermittelten Beiakte 001) nachgefragt, ob es sich dabei um eine Anhörung handelt oder nicht. Eine Anhörung besteht üblicherweise aus mindestens zwei Teilen: einer Sachverhaltsdarstellung und einer rechtliche Würdigung (Kallerhoff/Mayen in Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 10. Aufl. 2022, VwVfG § 28 Rn. 39 und 41; Schneider in Schoch/Schneider, Verwaltungsrecht - VwVfG, Werkstand: 7. EL Mai 2025, §28 Rn. 46; EuGH vom 21.11.1991 – C-269/90, Rn. 23 ff. = NVwZ 1992, 358; Nöhmer Anhörung im europ. VwVf, S. 241, 275).

Dem wurde keine Ihrer Mitteilungen gerecht und auch nicht die vorliegende Anhörung vom 27.01.2026. Bei mir entstand und besteht der Eindruck, Sie brauchen meine Unterstützung um den Sachverhalt zu ermitteln und rechtlich einzuordnen. Das kann ich gerne tun, aber dann möchte ich Ihnen eine Rechnung als Dienstleister schicken dürfen.

Für meine weitere Argumentation ist es wesentlich, dass das Beschwerdeverfahren nach meiner Auffassung in einen Verwaltungsakt mit Doppelwirkung (Laubinger, „Der Verwaltungsakt mit Doppelwirkung", Otto Schwarz Verlag & Co Göttingen 1967) bzw. mit Drittwirkung (Feuerstein, „Die Rechtsnatur des Verwaltungsaktes", Mohr-Siebeck Verlag 2025, Kapitel 11: Der Verwaltungsakt mit Drittwirkung) mündet. Nach Laubinger wir dieser wirksam mit Bekanntgabe an den belasteten, nach Feuerstein wird er wirksam jeweils mit der Bekanntgabe an den Beteiligten, allerdings bindet die erste Bekanntgabe die Verwaltung an den darin ausgedrückten Willen.

Nur leider ist Ihren Briefen jeglicher Hinweis darauf, dass es sich überhaupt um einen Verwaltungsakt handelt, insbesondere fehlt eine Kennzeichnung als z.B. Bescheid (§37 Abs. 1 VwVfG NRW) und eine für belastende Verwaltungsakte nach §37 Abs. 6 VwVfG NRW, für Beschwerdeabschlüsse aber auch durch Art. 77 DSGVO vorgeschriebene Rechtsbehelfsbelehrung. Mit anderen Worten, ihre Schreiben sind unwirksam und erfüllen damit weder meinen Anspruch aus Art. 77 DSGVO, noch den Durchsetzungsauftrag an Sie aus Art. 57 Abs. 1 lit. a DSGVO haben. Auch ist ein Hinweis nach Art. 58 Abs. 1 lit. d nicht das gebotene Instrument. Die DSGVO sieht für eine Beschwerde unterschiedliche

Instrumente in Art. 58 Abs. 2 DSGVO vor, insbesondere lit. c und d. Dass deutsche Datenschutzaufsichten selten Strafen verhängen ist bekannt, dass Sie daher kaum ernstgenommen werden auch.

Ihre Bescheide sind aber – bis auf die Ablehnung auch unbestimmt.

Lassen Sie mich zunächst die Beschwerden tabellarisch darstellen:

Datum		Mangel/Beschwerdeinhalt	Seite Beiakte	Vermutete Entscheidung		
Auskunftsersuchens	Beschwerde			Stattgabe	Unklar/offen	Ablehnung
19.02.2025	03.03.2025	formwidrige, unvollständige, und unverständliche Auskunft	1	nicht formgerecht, unvollständig	unverständlich?	
03.04.2025	12.05.2025	Auskunftsersuchen ignoriert (Punkt 3. der Email)	25	verfristet?	--	--
09.07.2025	05.08.2025	a) unvollständige Auskunft, b) fehlende Informationen bei gemeinsamer Verantwortlichkeit	104		a) unvollständig?	b) fehlende Informationen bei gemeinsamer Verantwortlichkeit?
16.10.2025	26.11.2025	a) unvollständige Auskunft, b) unsichere Kommunikation der Auskunft	223	--		unvollständig, unsichere Kommunikation

Klar ist Ihr Entwurf eigentlich nur dahingehend, dass Sie die Beschwerde vom 26.11.2025 ablehnen – zu Unrecht, dazu unten ausführlich. Zu den anderen Beschwerden schreiben Sie in Ihrem Entwurf „Darüber hinaus hat meine Prüfung zu Ihren Beschwerden vom 03.03.2025, 12.05.2025 und 05.08.2025 ergeben, dass die DPD Ihre Auskunftsanträge vom 20.02.2025 und daran anschließend die vom 03.04.2025 und 09.07.2025 nicht vollständig und zum Teil nicht formgerecht und verfristet beauskunftet hat.“ Ich halte diese Zusammenfassung für zu unbestimmt. Während Form und Frist noch einfach prüfbar sind, ist das bei unvollständig und unverständlich nicht zweifelsfrei möglich.

Konkret sind Sie nur zur „Unvollständigkeit der Auskünfte bezüglich des Nachsendeauftrages, der Ersatzzustellung und Postwurfspezial ist die DPD laut ihrer Stellungnahme vom 01.09.2025 nicht als die verantwortliche Stelle gemäß Art. 4 Nr. 7 DS-GVO anzusehen.“ Dass die Deutsche Post Direkt bei diesen Verarbeitungen wirklich nur Auftragsverarbeiter ist bezweifle ich sehr, ich darf hier um Wiederholungen zu vermeiden auf meine parallele Stellungnahme zur Anhörung vom 27.01.2026 in 21.40.2025-0008095 verweisen.

Durch Vergleich mit meinen zusammengefassten Beschwerdeinhalten in der Tabelle – die Sie aber nicht in den Bescheid aufgenommen haben – kann ich eine Vermutung hinsichtlich den stattgegebenen oder abgelehnten Beschwerdeanteilen aufstellen – aber es wäre Ihre Aufgabe, das konkret festzustellen und beiden Beteiligten zu kommunizieren. Das haben Sie nicht getan, und damit auch mit dem Inhalt gegen §37 Abs. 1 VwVfG NRW verstoßen. Da Sie manche Beschwerdeinhalte gar nicht aufführen ist unklar, ob diese Beschwerdeinhalte noch nicht entscheidungsreif waren oder ob Sie die unter den Tisch fallen lassen wollen.

Die Konsequenz dieser Mängel des Verwaltungsakts ist, dass es die Beschwerdegegnerin überhaupt nicht tangiert, denn der Verwaltungsakt entfaltet keine Wirkung. Genau das ist auch eingetreten, ich habe am 10.01.2026 eine weitere Auskunft bei der Beschwerdegegnerin angefordert und diese wurde erneut unvollständig beantwortet.

Bleibt noch die Ablehnung der Beschwerde vom 26.11.2025 (S. 223) zu kritisieren. Sie schreiben in Ihrer ablehnenden Email vom 10.12.2025 (S. 231f) „Die DPD hat mitgeteilt, dass die Abstimmung mit der Deutsche Post AG (DP AG) ohne Offenlegung personenbezogenen Daten erfolgt ist." Ich kann dazu keine Stellungnahme der Beschwerdegegnerin und auch keinen Vermerk in der Akte finden, Sie sind dieser Frage also nicht nachvollziehbar nachgegangen und haben damit wohl gegen §24 VwVfG NRW verstoßen. Sollte ich etwas übersehen haben, bitte ich um eine Seitenangabe der Akte. Aber auch dann bleibt der Hinweis auf das BGH Urteil vom 5. März 2024 - VI ZR 330/21:

> „Gemäß Art. 4 Nr. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ("betroffene Person") beziehen. **Nach der Rechtsprechung des Gerichtshofs der Europäischen Union ist der Begriff weit zu verstehen.** Er ist nicht auf sensible oder private Informationen beschränkt, sondern umfasst potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur, unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt. **Die letztgenannte Voraussetzung ist erfüllt, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist** (vgl. EuGH, Urteil vom 4. Mai 2023 - C-487/21, ...; Senatsurteil vom 15. Juni 2021 - VI ZR 576/19, NJW 2021, 2726 Rn. 22 mwN)."
> (BGH Urteil vom 5. März 2024 - VI ZR 330/21 Rn. 15, Hervorhebung durch den Kläger).

Es kommt also nicht darauf an, ob mein Name genannt wurde, sondern allein darauf, dass der Beschwerdeinhalt mit mir in Verbindung gebracht werden kann, was immer dann möglich ist, wenn nicht eine Vielzahl gleichartiger Beschwerden vorliegt. Dazu schreiben Sie nichts.

Völlig verfehlt ist die Ablehnung, weil das Datum der Auskunft als Schlüssel für eine Verschlüsselung denkbar ungeeignet ist. Schon eine Verwendung des Geburtsdatums hat der Landesbeauftragte für Datenschutz Baden-Württemberg als unsicher eingestuft (Anlage S1), dabei hat das Geburtsdatum einen Werteraum von ca. 50.000 verschiedenen Daten. Wenn man einen Aufbewahrungsfrist von Auskünften von typisch drei Jahren annimmt, dann sind das weniger als 1.100 verschiedene Daten, und der Schlüsselraum hat in etwa die Länge 10 Bit. Der Kläger hat ein Programm geschrieben, das einfach alle Daten vom Datum der Auskunftsdatei rückwärts durchprobiert hat, und es hat für das ¾ Jahr nur 30s gebraucht. Ist das Intervall kürzer, geht es schneller, mit mehr als 2 Minuten ist nicht zu rechnen. Und dabei war das Programm trivial und musste für jeden Test einen neuen Prozess anlegen, eine optimierte Version könnte ein Vielfaches schneller sein. Entsprechend schreibt der Landesbeauftragte für Datenschutz Baden-Württemberg, man könne heute Millionen von Passwörtern in wenigen Sekunden durchprobieren (Anlage S1, S. 6 unten).

Zum Vergleich: Bei der Verschlüsselung mit AES nach Stand-der-Technik werden Schlüssel mit mindestens 128 Bit verwendet, das ist etwa das 332.306.998.946.229.000.000.000.000.000.000.000 fache von 10Bit und die Suche nach dem richtigen Schlüssel würde sehr, sehr viel länger dauern, bei vergleichbarem Testprogramm ungefähr 1.263.620.803.658.940.000.000.000.000.000 Jahre.

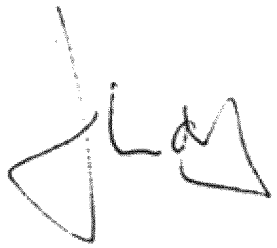
Es ist also entgegen der Darstellung der Beklagten, die Sie sich zu eigen machen, völlig irrelevant ob der Kläger Briefe mit oder ohne Datum veröffentlicht – durchprobieren ist trivial, und diese Art der Verschlüsselung daher unbrauchbar. Tatsächlich hat Herr Giese in seiner Antwort auf meine

Auskunftsanfrage vom 10.01.2026 ein falsches Datum eingesetzt – mein Programm hat weniger als 1s gebraucht, das verwendete Datum zu identifizieren (Anlagen S2 und S3).

Nur der Vollständigkeit halber: im Bescheid des LfDI BW ist die Rede von „ohne Transportverschlüsselung“ (Anlage S1 S.2 unten). Das ist wenig präzise, aber trifft es insofern auch im hier vorliegenden Fall als der Emailserver der Beigeladenen keine Transportverschlüsselung erzwingt und auch kein SMTP-DANE oder MTA-STS unterstützt (Anlage S4, Erläuterungen auf https://blog.lindenberg.one/EmailSicherheitsTest. Ausführlich zum Stand-der-Technik z.B. Lindenberg „Sichere Kommunikation per E-Mail“, DuD 2024, 726-732, abrufbar über https://blog.lindenberg.one/TopicEmailSicherheit).

Im Ergebnis bleibt mir festzustellen, dass Ihr Verfahren massive Verfahrensmängel und Mängel hinsichtlich der Feststellung der Sach- und Rechtslage aufweist. Ich fordere Sie daher auf, Ihren Bescheid vom 10.12.2025 – sofern man den überhaupt einen Bescheid nennen kann – an mich und an die Beschwerdegegnerin aufzuheben und das Beschwerdeverfahren entlang der oben aufgeworfenen Fragestellungen fortzusetzen

Vielen Dank und viele Grüße



Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

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

Per Einschreiben gegen Rückschein:

[redacted]
76227 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)

Datenschutzaufsichtsbehördliches Verfahren: Übermittlung von Corona-Testergebnissen
Unser Schreiben vom 3. April 2023
Ihr Schreiben vom „28.04.2022" (Eingegangen bei uns am 3. Mai 2023)

Sehr geehrte [redacted],

gegenüber der „[redacted] 76227 Karlsruhe erlässt der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (Aufsichtsbehörde) folgende datenschutzrechtliche

Verfügung:

1. Gegen die [redacted] wird wegen Verstoßes gegen Artikel 5 Absatz 1 Buchstabe f, Artikel 25 Absatz 1 und Artikel 32 Absatz 1 Satz 1 DS-GVO aufgrund der Übermittlung von Testergebnissen über das Coronavirus SARS-CoV-2 in einem unzureichend geschützten PDF-Dokument per E-Mail, eine **Verwarnung** nach Artikel 58 Absatz 2 Buchstabe b der Datenschutz-Grundverordnung (DS-GVO) ausgesprochen.

2. Für diese Verfügung wird eine Verwaltungsgebühr i. H. v. 400,00 Euro festgesetzt.

Begründung:

I. Sachverhalt

Wir haben folgenden Sachverhalt festgestellt:

Als Apotheke ([redacted], 76227 Karlsruhe) haben Sie bis November 2022 Ihren Kunden angeboten, Tests auf das Coronavirus SARS-CoV-2 durchzuführen. Nach den durchgeführten Tests wurden die Testergebnisse in einem passwortgeschützten PDF-Dokument per E-Mail an die getesteten Personen geschickt. Die Kunden haben das Passwort separat bei der Anmeldung erhalten. Als Passwort haben Sie das Geburtsdatum der getesteten Person verwendet. Für die Verarbeitung der Testdaten setzten Sie die Cloud-Dienste des Dienstleisters „No-Q GmbH" ein. Nach Ihren Angaben wurde das Testergebnis verschlüsselt übermittelt und war damit nur für den Kunden über den persönlichen E-Mail-Account zugänglich. Sie haben für die Kunden, die keine digitale Anmeldung vor Ort wünschten, die Mitteilung des Testergebnisses über das Coronavirus SARS-CoV-2 in Papierform vorgesehen.

Der Beschwerdeführer, Herr Joachim Lindenberg, hat sich bei uns über mangelhafte technisch und organisatorische Maßnahmen hinsichtlich des E-Mail-Versands beschwert und bezog sich dabei auf mehrfach bei Ihnen durchgeführte Corona-Tests einschließlich der Mitteilung des Testergebnisses. Nach ihrer telefonischen Kontaktaufnahme mit dem Beschwerdeführer haben Sie auf Rückfrage erfahren, dass dieser die Mitteilung des Testergebnisses in Papierform nicht wünschte. Dabei teilte der Beschwerdeführer mit, dass es ihm um das Problem der Verschlüsselung von Datenverarbeitungen als Grundsatzthematik in Deutschland gehe und bei der Übermittlung per E-Mail ohne Transportverschlüsselung ein Geburtsdatum nicht als Passwort dienen dürfe.

Der Beschwerdeführer vertritt die Auffassung, dass das Geburtsdatum leicht zu erraten oder ggf. bekannt sei und damit ein unzureichendes Passwort für den Schutz eines PDF-Dokuments darstelle und die Übermittlung der Testergebnisse per E-Mail ohne Transportverschlüsselung die Anforderungen des Artikels 32 DS-GVO nicht erfülle. Der Beschwerdeführer vertieft seine Ausführungen dahingehend, dass der von der Beschwerdegegnerin eingesetzte Dienstleister No-Q GmbH für den E-Mail-Ver-

sand keine qualifizierte Transportverschlüsselung eingesetzt habe, was der Beschwerdeführer mit einer von ihm verwendeten speziellen E-Mail-Adresse feststellen könne. Der Versand der E-Mails erfolge zwar dann auf dem Transportweg verschlüsselt, wenn der E-Mail-Server des Empfängers eine Transportverschlüsselung unterstütze. Das E-Mail-System des Beschwerdeführers als Empfänger der E-Mails hat die Transportverschlüsselung jedoch nicht unterstützt und E-Mails waren nur unverschlüsselt zustellbar. Stattdessen hätte die Beschwerdegegnerin über den er absendende E-Mail-Server für die abgesendeten E-Mails den Versand ohne Transportverschlüsselung nicht durchführen dürfen.

Sie tragen vor, dass Sie in Anbetracht der hohen Sicherheitsanforderungen für die Verarbeitung der Testergebnisse über das das Coronavirus SARS-CoV-2 einen professionellen und renommierten Anbieter „No-Q GmbH" ausgewählt hätten, dessen bereitgestellte Software 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. Zuständigkeit

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg ist örtlich gemäß § 19 Absatz 2 Satz 1 des Bundesdatenschutzgesetzes (folgend: BDSG) und § 3 Absatz 1 Nr. 3 Buchstabe b des Landesverwaltungsverfahrensgesetzes und sachlich nach Artikel 51 Absatz 1 DS-GVO und § 40 Absatz 1 BDSG sowie § 25 Absätze 1 und 2 des Landesdatenschutzgesetzes die zuständige Datenschutzaufsichtsbehörde für den Erlass einer Verwarnung.

III. Rechtliche Bewertung

1. Datenschutzrechtliche Verantwortlichkeit

Über die [redacted] haben Sie Testungen auf das Coronavirus SARS-CoV-2 in eigener datenschutzrechtlicher Verantwortung nach Artikel 4 Nummer 7 DS-GVO angeboten. Dabei haben Sie über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entschieden und Dienstanbieter No-Q GmbH als Auftragsverarbeiter nach Artikel 28 DS-GVO für die durchgeführten Testungen auf das Coronavirus SARS-CoV-2 eingesetzt.

2. Technische und Organisatorische Maßnahmen

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.

a. 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, Absender und Empfänger erkennen.

Mit der Transportverschlüsselung wird die laufende Kommunikation während der 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 erkennbar ist. Ob eine Transportverschlüsselung zum Einsatz kommt und die Art des Verschlüsselungsverfahrens, unterliegt der technischen Aushandlung zwischen den beteiligten E-Mail-Servers. 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 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.
- Etwas höhere Sicherheit bietet die *obligatorische Transportverschlüsselung*: Wenn keine Verschlüsselung zustande kommt, lehnt der E-Mail-Server, der obligatorische Transportverschlüsselung erfordert (also Sender oder Empfänger), die weitere Übermittlung ab. Die E-Mail ist in diesem Fall nicht zustellbar.

- Bei der *qualifizierten Transportverschlüsselung* prüfen Sender und/oder Empfänger zusätzlich, ob es sich bei der Gegenstelle tatsächlich um die korrekte Gegenstelle handelt. Andernfalls wird die Zustellung abgebrochen, die E-Mail kann also nicht zugestellt werden.

Die große 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 gegenüber der Sicherheit vorrangig ist.

Demgegenüber dient eine Inhalts- oder Ende-zu-Ende-Verschlüsselung dafür, Teile oder alle Inhalte einer E-Mail zu verschlüsseln. Dies geschieht vollständig unabhängig vom Transportweg und von der Transportverschlüsselung. Der Vorteil ist, dass die auf diese Weise verschlüsselten Inhalte auch vor Einblicken der beteiligten E-Mail-Dienstanbieter oder erfolgreichen Angreifern 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 wie insbesondere über die Sender und Empfänger. Zudem erfordert es eine Unterstützung durch Empfänger und Sender, nicht nur der im Hintergrund beteiligten Dienstleister.

- 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 Geburtsdatum als Passwort per E-Mail

Das von Ihnen für die Übermittlung der Testergebnisse verwendete E-Mail-System sieht die sogenannte opportunistische Transportverschlüsselung vor. Für die Inhaltsverschlüsselung haben Sie PDF-Dateien verwendet, für deren Schutz das Geburtsdatum der Testperson als Passwort zum Einsatz kam.
Darin liegt ein Verstoß gegen den einzuhaltenden Stand der Technik nach Artikel 25 Absatz 1, 32 Absatz 1 Buchstabe a DS-GVO und eine Verletzung des Grundsatzes der Vertraulichkeit und Integrität nach Artikel 5 Absatz 1 Buchstabe f DS-GVO. 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, die eine Datenschutz-Folgenabschätzung voraussetzen, vgl. Artikel 35 Absatz 3 Buchstabe b DS-GVO. Nach Artikel 32 Absatz 1 Buchstabe a DS-GVO sind daher die Testergebnisse über das Coronavirus SARS-CoV-2 verschlüsselt zu übermitteln, und ein ausreichender Schutz vor und nach dem eigentlichen Transportweg vorzusehen. Demnach ist der von Ihnen 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 einer passwortgeschützten PDF-Datei 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 kommendes Passwort. 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 sind Sie gesetzlich gehalten selbst und über den Auftragsverarbeiter, die mit der Verarbeitung der Testergebnisse verbundenen hohen Risiken hinreichend zu mindern. Sie müssen 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, unter https://lfdi-bw.de/dsk-oh-email.

Damit die Transportverschlüsselung wirken kann, ist es nötig, dass sowohl Ihr E-Mail-Ausgangsserver als auch der E-Mail-Eingangsserver des Beschwerdeführers als Empfänger der E-Mail ausreichende technische Maßnahmen durchführen. Dabei liegt zwar die Verantwortung für den sicheren Versand der E-Mail bei Ihnen als Senderin und gleichzeitig ist der Empfänger gehalten die technischen Voraussetzungen für einen sicheren Empfang der E-Mail vorzusehen. Wenn Sie die obligatorische Transportverschlüsselung oder qualifizierte Transportverschlüsselung vorgesehen hätten, wäre es nicht möglich gewesen, dem Beschwerdeführer das Testergebnis per E-Mail zu übermitteln. Insofern steht der Beitrag des Beschwerdeführers hinsichtlich seines Schutzes als betroffene Person im Sinne eines Selbstdatenschutzes in Frage, zumal er die Mitteilung des Testergebnisses in Papierform ausdrücklich nicht wünschte und mit seinem Vorgehen feststellen konnte, ob Sie E-Mails auch ohne Transportverschlüsselung zustellen. Bei der Abwägung über die Zulässigkeit der durchgeführten technischen Maßnahmen ist auch zu bewerten, welche Folgen eine obligatorische (oder gar qualifizierte) Transportverschlüsselung hätte: Diese würde dafür sorgen, dass E-Mails mit dem Ergebnis des Corona-Tests nicht zugestellt werden könnten und im besten Falle würde die Teststelle eine Fehlermeldung über die Unzustellbarkeit erhalten. Dies würde der Erwartungshaltung der Empfänger als auch 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 Tests 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.

Schließlich weisen wir darauf hin, dass die Corona-Warn-App eine Funktionalität vorsah, um die Testergebnisse auf das das Coronavirus SARS-CoV-2 gesichert zu übermitteln und in der Applikation abzurufen. Damit wäre eine sichere Übermittlung gewährleistet gewesen, vgl. https://www.coronawarn.app/de/faq/results/?search=&topic=application.

IV. Sanktion

1. Ermächtigungsgrundlage

Hat die Aufsichtsbehörde einen Verstoß gegen eine Regelung der DS-GVO festgestellt, kann sie gegenüber der verantwortlichen Stelle eine Anordnung nach Artikel 58 Absatz 2 Buchstabe a bis g DS-GVO in Form eines Verwaltungsaktes erlassen. In Anbetracht des in der Vergangenheit liegenden Verstoßes gegen die Datenschutz-Grundverordnung hat sich die Aufsichtsbehörde entschieden, Ihnen gegenüber eine Verwarnung nach Artikel 58 Absatz 2 Buchstabe b DS-GVO auszusprechen. Nach dieser Vorschrift hat die Aufsichtsbehörde die Möglichkeit, eine für die Verarbeitung personenbezogener Daten verantwortliche Stelle zu verwarnen, wenn diese mit den Datenverarbeitungsvorgängen gegen die DS-GVO verstoßen hat. Wie oben unter Nr. III. ausgeführt, liegt ein solcher Verstoß in dem beschwerdegegenständlichen Sachverhalt zum Nachteil des Beschwerdeführers aber auch anderer betroffener Personen vor.

2. Ermessensausübung: Verhältnismäßigkeit

Der Erlass einer Verwarnung unterliegt dem pflichtgemäßen Ermessen der Datenschutzaufsichtsbehörde (vgl. dazu VG Stuttgart, Urteil vom 11. November 2021 - 11 K 17/21 - BeckRS 2021, 55554; Will, ZD 2020, 97).

Nach dem Erwägungsgrund 148 der DS-GVO sollen die Datenschutzaufsichtsbehörden berücksichtigen, dass im Interesse einer konsequenten Durchsetzung der Verordnung bei Verstößen zusätzlich oder anstelle von sogenannten geeigneten Maßnahmen (Anweisungen oder Anordnungen) auch Sanktionen (Verwarnungen oder Geldbußen) verhängt werden sollen. Die Verwarnung ist dabei aus Sicht des europäischen Gesetzgebers als eine gegenüber der Geldbuße mildere Sanktion für erstmalige oder nicht in besonderer Weise gravierende Verstöße vorgesehen und dient general- und spezialpräventiven Ahndungszwecken. Sie ist für Sachverhalte geeignet, die in der Vergangenheit liegen und von denen keine potentielle Verletzung des Schutzes personenbezogener Daten nach Artikel 8 der Charta der Grundrechte der Europäischen Union und des Rechts auf informationelle Selbstbestimmung nach Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 des Grundgesetzes mehr ausgeht. Da die verantwortliche Stelle seit November 2022 keine Testungen auf das Coronavirus SARS-CoV-2 mehr durchführt, hat sich der beschwerdegegenständliche Sachverhalt erledigt. Gleichzeitig ist auf der Webseite der verantwortlichen Stelle erkennbar, dass diese weiterhin den Auftragsverarbeiter „No-Q GmbH" einsetzt für Buchungssystem/Ergebnisübermittlung, vgl. Webseite, abrufbar unter: https://www.eisbaerapotheke.de/datenschutz.php.

Insofern ist die Verwarnung im Hinblick auf potentielle andere Sachverhalte ein geeignetes Mittel. Zwar ist zu Lasten der verantwortlichen Stelle festzustellen, dass eine erhebliche eine Schwere des Verstoßes gegen die Datenschutz-Grundverordnung hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen nach Artikel 25 Absatz 1 und Artikel 32 Absatz 1 Buchstabe b DS-GVO bei der Verarbeitung von Gesundheitsdaten bestand, worin eine Verletzung des Grundsatzes der Vertraulichkeit und Integrität nach Artikel 5 Absatz 1 Buchstabe f DS-GVO lag. Gleichzeit handelt es sich um eine zeitlich beschränkte Dauer des Verstoßes, so dass es sich bei der Verwarnung um das relativ mildeste Mittel, zumal vergleichbare Konstellationen der Testungen auf das Coronavirus SARS-CoV-2 derzeit nicht erkennbar sind. Ferner ist nicht ersichtlich, dass zwischen dem Ziel einer Sanktionierung, dem Mittel und den möglichen Folgen der Verwarnung ein offensichtliches Missverhältnis bestünde. Daher stellt die Verwarnung im Verhältnis zur Schwere des in der Vergangenheit liegenden Verstoßes ein angemessenes Mittel dar.

V. Kosten

Die Verwaltungsgebühr richtet sich nach § 1 der Gebührenverordnung Landesbeauftragter für den Datenschutz und die Informationsfreiheit (GebVO LfDI) und Nr. 2.2.1

des diesbezüglichen Gebührenverzeichnisses (GebVerz LfDI), wonach eine Rahmengebühr von 100,00 € bis 5.000,00 € vorgesehen ist. Ein Betrag von 400,00 € ist angesichts des dargelegten Sach- und Streitstandes, des tatsächlichen Aufwands sowie unter Zugrundelegung eines Pauschalsatzes je Arbeitsstunde von 89 € im höheren Dienst gem. Nummer 2.1 der Verwaltungsvorschrift des Finanzministeriums über die Berücksichtigung der Verwaltungskosten insbesondere bei der Festsetzung von Gebühren und sonstigen Entgelten für die Inanspruchnahme der Landesverwaltung angemessen.

Nach Bestandskraft der Verfügung wird Ihnen eine gesonderte Zahlungsaufforderung mit Buchungszeichen und Buchungsempfänger zugehen.

VI. Rechtsbehelfsbelehrung

Gegen diesen Bescheid kann binnen eines Monats nach dessen Bekanntgabe Klage beim Verwaltungsgericht Stuttgart, Augustenstr. 5, 70178 Stuttgart (Postanschrift: Postfach 10 50 52, 70044 Stuttgart, Fax-Nrn.: 0711 / 6673-6801 oder 0711 / 6673-6970) erhoben werden.

Mit freundlichen Grüßen

Im Auftrag

[redacted]

Anlage S2

Joachim Lindenberg

Von: Joachim Lindenberg <[redacted]@lindenberg.one>
Gesendet: Freitag, 23. Januar 2026 15:57
An: '[redacted] (Deutsche Post Direkt), external'
Betreff: AW: Deutsche Post Direkt GmbH - Ihr Auskunftsverlangen

Sehr geehrter [redacted],
vielen Dank für Ihre Auskunft. Aber auch diesmal gibt es einiges zu kritisieren:

- Ich kann mich nicht erinnern, am 15.01.2026 ein Auskunftsersuchen gestellt zu haben. Aber da Sie eine unsinnige Schlüssel für die Verschlüsselung verwenden, konnte mein Programm das Datum und damit den Schlüssel in weniger als einer Sekunde ermitteln.
- Ihre Auskunft ist nicht korrekt, oder wieso steht in der Auskunft „Aufgrund Ihrer in den Datenbeständen von Post Direkt bislang nicht gespeicherten E-Mail-Adresse ist eine Authentifizierung Ihrer Person nicht möglich und erhalten Sie die Auskunft/Sperrbestätigung per Post."
- Ihre Auskunft ist unvollständig. Haben Sie kein Verzeichnis der Verarbeitungstätigkeiten oder verwenden Sie es trotz der Übereinstimmungen von Artikel 13-15 und 30 DSGVO nicht? Ich vermisse zumindest die Informationen die ich mit dem Support der Post Direkt ausgetauscht habe. Welche Verfahren und Datenarten haben Sie noch weggelassen?
- Sie haben nur die letzten beiden Schreiben der LDI beauskunftet und auch sonst fehlen Teile der vorhergehenden Auskünfte. Da ich um eine vollständige Auskunft gebeten habe (meine Email vom 10.01.2026), habe ich Anspruch auf alle Daten, die Gegenstand der Verarbeitung sind (Art. 15 Abs. 3 Satz 1) , also insbesondere alle, die gespeichert werden (Art. 4 Nr. 2 DSGVO). Wieso lassen Sie ohne mein Einverständnis Teile der Datenkopie weg?
- Ihre Angaben nach Art. 15 Abs. 1 sind unvollständig. Sie schreiben unten: „Wir werden Ihre Daten in der Datenbank für den Adressabgleich zum Ablauf des 02.02.2026 löschen.“? Das hat mich stutzig gemacht: Ergibt sich das aus einer Speicherfrist in der Auskunft? Hab ich einen Antrag nach Art. 17 DSGVO gestellt? Oder ist das Willkür? Natürlich habe ich nach entsprechenden Angaben in Ihrer Auskunft gesucht und stelle fest, dass die nach Art. 15 Abs. 1 geforderten Angaben sehr unvollständig sind, insbesondere finde ich keine Speicherdauern. Auch Empfänger verschweigen Sie erneut.

Ich darf Sie auffordern, zeitnah eine vollständige Auskunft zu erteilen.
Vielen Dank und viele Grüße
Joachim Lindenberg

Von: [redacted](Deutsche Post Direkt), external <[redacted].extern@postdirekt.de>
Gesendet: Donnerstag, 22. Januar 2026 18:26
An: [redacted]@lindenberg.one
Cc: Datenschutz (Post Direkt) <datenschutz@postdirekt.de>
Betreff: Deutsche Post Direkt GmbH - Ihr Auskunftsverlangen

Sehr geehrter Herr Lindenberg,

in der Anlage erhalten die gewünschte Auskunft nach Art. 15 DSGVO.
In der ZIP-Datei finden Sie
- das Auskunftsschreiben von Post Direkt mit Datum vom 22.01.2026,
- die weitere Korrespondenz der LDI NRW mit Post Direkt.

Die ZIP-Datei ist mittels Passworts geschützt. Das Passwort ist das Datum des letzten Auskunftsersuchens von Ihnen an Post Direkt in der Schreibweise tt.mm.jjjj.

Wir werden Ihre Daten in der Datenbank für den Adressabgleich zum Ablauf des 02.02.2026 löschen.

Anlage S3

Joachim Lindenberg

Von: [redacted] (Deutsche Post Direkt), external <[redacted].extern@postdirekt.de>
Gesendet: Montag, 26. Januar 2026 17:25
An: Joachim Lindenberg
Betreff: AW: Deutsche Post Direkt GmbH - Ihr Auskunftsverlangen

Sehr geehrter Herr Lindenberg,

in der Tat datiert Ihr Auskunftsersuchen an datenschutz@postdirekt.de nicht auf den 15.01.2026, sondern auf den 10.01.2026. Dies war ein Schreibfehler meinerseits.

Die Korrespondenz mit der Aufsichtsbehörde LDI NRW habe ich Ihnen vollständig zusammen mit der Auskunft vom 27.10.2025 übersandt.
Sofern in dem aktuell übersandten Schreiben der LDI NRW, Referat 24, vom 10.12.2025 Bezug genommen wird auf ein Schreiben von mir vom „16.10.2025" ist dies ein Schreibfehler. Mein Schreiben an das Referat 24 datiert auf den 15.10.2025 und liegt Ihnen bereits vor.

In den Posteingangsfächern des Kundenservice/Kundenmanagement info@... kundenmanagement@... und support@... der Post Direkt können wir keine E-Mail von Ihnen finden. Wir bitten insoweit um Konkretisierung.

Zu den weiteren Fragen/Anmerkungen von Ihnen nehme ich gerne noch Stellung.

Mit freundlichen Grüßen

[redacted]
Rechtsanwalt und
Externer Datenschutzbeauftragter Deutsche Post Direkt GmbH und Deutsche Post Dialog Solutions GmbH

Kanzlei-Anschrift und Kontaktdaten:
[redacted]
Telefon +49 228 [redacted]
Telefax +49 228 [redacted]
Mobil +49 171 [redacted]
E-Mail [redacted].extern@postdirekt.de
E-Mail [redacted]

Anlage S4

Verbindungshistorie

14.12.2025 22:07:59 - 22:08:11 (gateway1c.dhl.com/gateway1c.dhl.com/165.72.200.98/DHLNET-165-72, DHL Information Services (Europe) s.r.o, Czech Republic -> Server 2, nicht verschlüsselt, Connect):
From: <p***y@postdirekt.de> To: <nr@et.lindenberg.one>
Id:446879088.284.1765746479188@vld1064.postdirekt.bprod Spf:Pass Signatures:Dkim
14.12.2025 22:08:05 - 22:08:16 (gateway1c.dhl.com/gateway1c.dhl.com/165.72.200.98/DHLNET-165-72, DHL Information Services (Europe) s.r.o, Czech Republic -> Server 2, nicht verschlüsselt, Connect):
From: <p***y@postdirekt.de> To: <nr@et.lindenberg.one>
Id:446879088.284.1765746479188@vld1064.postdirekt.bprod Spf:Pass Signatures:Dkim
14.12.2025 22:08:11 - 22:08:21 (gateway1c.dhl.com/gateway1c.dhl.com/165.72.200.98/DHLNET-165-72, DHL Information Services (Europe) s.r.o, Czech Republic -> Server 2, nicht verschlüsselt, Connect):
From: <p***y@postdirekt.de> To: <nr@et.lindenberg.one>
Id:446879088.284.1765746479188@vld1064.postdirekt.bprod Spf:Pass Signatures:Dkim
14.12.2025 22:08:16 - 22:08:22 (gateway1c.dhl.com/gateway1c.dhl.com/165.72.200.98/DHLNET-165-72, DHL Information Services (Europe) s.r.o, Czech Republic -> Server 2, nicht verschlüsselt, Connect):
From: <p***y@postdirekt.de> To: <nr@et.lindenberg.one>
Id:446879088.284.1765746479188@vld1064.postdirekt.bprod Spf:Fail Signatures:Dkim
14.12.2025 22:14:19 - 22:14:31 (gateway1c.dhl.com/gateway1c.dhl.com/165.72.200.98/DHLNET-165-72, DHL Information Services (Europe) s.r.o, Czech Republic -> Server 6, verschlüsselt mit TLS 1.3, Mail):
From: <p***y@postdirekt.de> To: <nr@et.lindenberg.one>
Id:446879088.284.1765746479188@vld1064.postdirekt.bprod Spf:Pass Signatures:Dkim
14.12.2025 22:14:25 - 22:14:37 (gateway1c.dhl.com/gateway1c.dhl.com/165.72.200.98/DHLNET-165-72, DHL Information Services (Europe) s.r.o, Czech Republic -> Server 6, verschlüsselt mit TLS 1.3, Mail):
From: <p***y@postdirekt.de> To: <nr@et.lindenberg.one>
Id:446879088.284.1765746479188@vld1064.postdirekt.bprod Spf:Pass Signatures:Dkim
14.12.2025 22:14:37 - 22:14:42 (gateway1c.dhl.com/gateway1c.dhl.com/165.72.200.98/DHLNET-165-72, DHL Information Services (Europe) s.r.o, Czech Republic -> Server 4, verschlüsselt mit TLS 1.3, Mail):
From: <p***y@postdirekt.de> To: <nr@et.lindenberg.one>
Id:446879088.284.1765746479188@vld1064.postdirekt.bprod Spf:Pass Signatures:Dkim
14.12.2025 22:14:31 - 22:14:42 (gateway1c.dhl.com/gateway1c.dhl.com/165.72.200.98/DHLNET-165-72, DHL Information Services (Europe) s.r.o, Czech Republic -> Server 6, verschlüsselt mit TLS 1.3, Mail):
From: <p***y@postdirekt.de> To: <nr@et.lindenberg.one>
Id:446879088.284.1765746479188@vld1064.postdirekt.bprod Spf:Pass Signatures:Dkim
14.12.2025 22:20:55 - 22:21:06 (gateway1c.dhl.com/gateway1c.dhl.com/165.72.200.98/DHLNET-165-72, DHL Information Services (Europe) s.r.o, Czech Republic -> Server 5, verschlüsselt mit TLS 1.3, Mail):
From: <p***y@postdirekt.de> To: <nr@et.lindenberg.one>
Id:446879088.284.1765746479188@vld1064.postdirekt.bprod Spf:Fail Signatures:Dkim
14.12.2025 22:21:00 - 22:21:42 (gateway1c.dhl.com/gateway1c.dhl.com/165.72.200.98/DHLNET-165-72, DHL Information Services (Europe) s.r.o, Czech Republic -> Server 3, verschlüsselt mit TLS 1.3, Mail):
From: <p***y@postdirekt.de> To: <nr@et.lindenberg.one>
Id:446879088.284.1765746479188@vld1064.postdirekt.bprod Spf:Fail Signatures:Dkim
14.12.2025 22:21:06 - 22:21:42 (gateway1c.dhl.com/gateway1c.dhl.com/165.72.200.98/DHLNET-165-72, DHL Information Services (Europe) s.r.o, Czech Republic -> Server 3, verschlüsselt mit TLS 1.3, Acked):
From: <p***y@postdirekt.de> To: <nr@et.lindenberg.one>
Id:446879088.284.1765746479188@vld1064.postdirekt.bprod Spf:Pass Signatures:Dkim

Analyse Senden von Email

Alle Mailserver erhielten Post, auch die mit ungültigen Zertifikaten (Postfix: may).
Ihr Mailserver verwendet kein SNI, also auch kein RFC 7672 oder RFC 8461.
Ihr Mailserver hat eine Mail (FROM/RCPT/DATA) ohne Verschlüsselung (STARTTLS) übertragen. Selbst wenn er RFC 7672 oder RFC 8461 verwenden sollte, erzwingt er keine Verschlüsselung (nicht gut, aber leider normal).
Einige Mails scheiterten an der Authentifizierung mit DKIM oder SPF - möglicherweise Spam.
Der Mailanbieter offenbart unnötig die folgenden IP-Adressen: 192.168.188.10

Analyse Empfangen von Email

	Mailserver (Prio)	Adresse(n)	Aussteller Rootzertifikat	DNSSEC	STARTTLS	TLS Version	Zertifikat	Passende TLSA	MTA-STS
	dhl-com.fortimailcloud.com (5)	154.52.2.252, 154.52.13.119	DigiCert Global Root G2	—	Erfolgreich	1.3	Vertrauenswürdig	Keine	Keine Policy
X	Qualifizierte Transportverschlüsselung			X	✓	✓			
X	RFC 7672 SMTP-DANE			X	✓	✓		X	
X	RFC 8461 MTA-STS				✓	✓	✓		X

	Summary	✗	✓	✓	✓	✗	✗
	Netzwerkinformationen						
	COGENT-154-52-16, Cogent Communications, LLC, United States : 154.52.0.0/16						
	DHLNET-165-72, DHL Information Services (Europe) s.r.o, Czech Republic : 165.72.0.0/16						

Die eingehende Authentfizierung von postdirekt.de wurde noch nicht getestet.

Mehr Informationen ggfs. auf https://blog.lindenberg.one/EmailSicherheitsTest#postdirekt.de