Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Vodafone GmbH
Datenschutzbeauftragter
Herr Dr. Herkströter
Ferdinand-Braun-Platz 1
40549 Düsseldorf

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-[redacted]
E-MAIL Referat24@bfdi.bund.de
BEARBEITET VON [redacted]
INTERNET www.bfdi.bund.de
DATUM Bonn, 11.04.2023
GESCHÄFTSZ. 24-193 II#6079

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Datenschutz in der Telekommunikation, Az. 24-193 II#6079**

Sehr geehrtes Vodafone Datenschutzteam,

mir liegt eine neue Eingabe zu Datenschutzfragen betreffend Ihr Unternehmen vor. Dieses wird hier unter dem oben genannten Geschäftszeichen geführt. Bitte geben Sie im nachfolgenden Schriftverkehr zu dieser Angelegenheit immer dieses Geschäftszeichen an. Die Eingabe kommt von folgender Person:

Herrn
Joachim Lindenberg
Heubergstr. 1a
76228 Karlsruhe

E-Mail: [redacted]@lindenberg.one

Der Beschwerdeführer B moniert einen Verstoß gegen Artikel 32 DSGVO, weil Vodafone bei der Registrierung von Kundenzugängen keine obligatorische E-Mail-Verschlüsselung verwendet.

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Der Beschreibung nach hat B unter

https://www.vodafone.de/meinvodafone/account/registrierung/persoenliche_daten

auf „ich bin noch kein Kunde“ geklickt und anschließend einen Vodafone Account angelegt. Daraufhin hat er eine Registrierungs-E-Mail erhalten. Mit einem Mail-Testprogramm hat B anschließend die unter tbpa.vodafone.de und kundenservice.vodafone.com erreichbaren Mailserver auf die eingesetzten Verschlüsselungsmechanismen untersucht und dabei festgestellt, dass die Mailserver Transportverschlüsselung mittels TLS unterstützen, diese Verschlüsselung jedoch nicht obligatorisch konfiguriert ist. Die Ergebnisse des Tests finden sie als Anlage anbei.

Durch eine obligatorische Transportverschlüsselung soll eine unverschlüsselte Übermittlung der Nachrichten ausgeschlossen werden. Sie kann über das Protokoll SMTPS oder durch Aufruf des SMTP-Befehls STARTTLS und den nachfolgenden Aufbau eines mit dem Protokoll TLS verschlüsselten Kommunikationskanals realisiert werden, wobei die Anforderungen der BSI TR 02102-2 zu erfüllen sind. Unterstützt die Gegenstelle kein TLS, dann wird der Verbindungsaufbau abgebrochen.

Zur Erläuterung:

Gemäß der Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021 zum Thema "Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail" müssen Verantwortliche, die gezielt personenbezogene Daten per E-Mail entgegennehmen, die Voraussetzungen für den sicheren Empfang von E-Mail-Nachrichten per TLS schaffen.

Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei denen der Bruch der Vertraulichkeit sogar ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er sowohl qualifizierte Transportverschlüsselung als auch den Empfang von Ende zu Ende verschlüsselter Nachrichten ermöglichen. Außerdem müssen bestehende PGP- oder S/MIME-Signaturen dann qualifiziert geprüft werden.

Beim Versand von E-Mail-Nachrichten mit personenbezogenen Daten, bei denen ein Bruch der Vertraulichkeit (des Inhalts oder Umstände der Kommunikation, soweit sie sich auf natürliche Personen beziehen) ein Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, sollten sich an der TR 03108-1 orientieren und müssen eine obligatorische Transportverschlüsselung sicherstellen.

Verantwortliche, die E-Mail-Nachrichten versenden, bei denen ein Bruch der Vertraulichkeit von personenbezogenen Daten im Inhalt der Nachricht ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, müssen regelmäßig eine Ende-zu-Ende-Verschlüsselung und eine qualifizierte Transportverschlüsselung vornehmen. Inwieweit entweder auf die Ende-zu-Ende-Verschlüsselung oder die Erfüllung einzelner Anforderungen an diese oder an die qualifizierte Transportverschlüsselung (z. B. DANE oder DNSSEC) verzichtet werden kann, hängt von den bestehenden Risiken, der konkreten Ausgestaltung des Übertragungsweges und ggf. getroffenen kompensierenden Maßnahmen ab.

Zum Schutz der Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten müssen öffentliche E-Mail-Diensteanbieter zudem die Anforderungen der BSI TR 03108-1 einhalten.

Ich bitte um sachliche und rechtliche Stellungnahme innerhalb von 4 Wochen.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Von: Lindenberg Email Test Service (emailtest@lindenberg.one)
An: emailtest@lindenberg.one (emailtest@lindenberg.one)
Gesendet: Mo 20.03.2023 15:21
Betreff: Test result for tbpa.vodafone.de, kundenservice.vodafone.com

Connection History:
03.20.2023 14:14:11 - 14:14:15 (demta3hr.tbpa.vodafone.de/demta3hr.tbpa.vodafone.de/::ffff:139.7.147.215 -> Server 7, plain text, None):
From: <b***e@kundenservice.vodafone.com> To: <nr@ut.lindenberg.one> Signatures:Dkim
03.20.2023 14:19:48 - 14:19:52 (demta2hr.tbpa.vodafone.de/demta2hr.tbpa.vodafone.de/::ffff:139.7.147.214 -> Server 2, plain text, None):
From: <b***e@kundenservice.vodafone.com> To: <nr@et.lindenberg.one> Signatures:Dkim
03.20.2023 14:20:19 - 14:20:23 (demta2hr.tbpa.vodafone.de/demta2hr.tbpa.vodafone.de/::ffff:139.7.147.214 -> Server 7, plain text, None):
From: <b***e@kundenservice.vodafone.com> To: <nr@ut.lindenberg.one> Signatures:Dkim
03.20.2023 14:20:47 - 14:20:51 (demta4hr.tbpa.vodafone.de/demta4hr.tbpa.vodafone.de/::ffff:139.7.147.216 -> Server 2, plain text, None):
From: <b***e@kundenservice.vodafone.com> To: <nr@et.lindenberg.one> Signatures:Dkim
03.20.2023 14:21:06 - 14:21:10 (demta2hr.tbpa.vodafone.de/demta2hr.tbpa.vodafone.de/::ffff:139.7.147.214 -> Server 7, encrypted, Mail):
From: <b***e@kundenservice.vodafone.com> To: <nr@ut.lindenberg.one> Signatures:Dkim
03.20.2023 14:21:17 - 14:21:21 (mtainet2.tbpa.vodafone.de/mtainet2.tbpa.vodafone.de/::ffff:139.7.147.197 -> Server 2, encrypted, Mail):
From: <b***e@kundenservice.vodafone.com> To: <nr@et.lindenberg.one> Signatures:Dkim
03.20.2023 14:27:34 - 14:27:39 (mtainet2.tbpa.vodafone.de/mtainet2.tbpa.vodafone.de/::ffff:139.7.147.197 -> Server 2, encrypted, Acked):
From: <b***e@kundenservice.vodafone.com> To: <nr@et.lindenberg.one> Signatures:Dkim
03.20.2023 14:28:05 - 14:28:10 (demta2hr.tbpa.vodafone.de/demta2hr.tbpa.vodafone.de/::ffff:139.7.147.214 -> Server 2, encrypted, Acked):
From: <b***e@kundenservice.vodafone.com> To: <nr@et.lindenberg.one> Signatures:Dkim
03.20.2023 14:29:08 - 14:29:12 (demta4hr.tbpa.vodafone.de/demta4hr.tbpa.vodafone.de/::ffff:139.7.147.216 -> Server 2, encrypted, Acked):
From: <b***e@kundenservice.vodafone.com> To: <nr@et.lindenberg.one> Signatures:Dkim
03.20.2023 14:31:00 - 14:31:04 (demta3hr.tbpa.vodafone.de/demta3hr.tbpa.vodafone.de/::ffff:139.7.147.215 -> Server 7, encrypted, Acked):
From: <b***e@kundenservice.vodafone.com> To: <nr@ut.lindenberg.one> Signatures:Dkim

Analysis Sending of Email
Your mailserver does not use SNI, hence does not support RFC 7672 nor RFC 8461, and likely accepts any certificate when sending (bad).
Your mailserver was sending a mail (FROM/RCPT/DATA) without using STARTTLS first. Even though it may support RFC 7672 or RFC 8461, it does not enforce encryption (bad, but kind of normal).

Analysis Reception of Email
Domain kundenservice.vodafone.com @ Provider vodafone.de does not use DNSSEC with MX-Records (bad).
Domain kundenservice.vodafone.com @ Provider vodafone.de does not use DNSSEC with A-Records (bad).
Domain kundenservice.vodafone.com @ Provider vodafone.de does not use DNSSEC with TLSA-Records (bad).
Domain kundenservice.vodafone.com @ Provider vodafone.de does support STARTTLS (good).
Domain kundenservice.vodafone.com @ Provider vodafone.de does not use valid certificates (bad).
Domain kundenservice.vodafone.com @ Provider vodafone.de does not support qualified transport encryption (bad).
Domain kundenservice.vodafone.com @ Provider vodafone.de does not support RFC 7672 SMTP-DANE (bad).
Domain kundenservice.vodafone.com @ Provider vodafone.de does not support RFC 8461 MTA-STS (bad).