Der Bayerische Landesbeauftragte für den Datenschutz

Bayer. Datenschutzbeauftragter • PF 22 12 19 • 80502 München

Frau Christina Franke
Hirschstraße [redacted]
76137 Karlsruhe

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen	München, den 26.09.2022
02.08.2022	DSB/7-193-580	Durchwahl: 089 212672 - 0

Sicherheit des Verwaltungsportals

Sehr geehrte Frau Franke,

vielen Dank für Ihr Schreiben vom 2. August 2022, in dem Sie noch einmal folgende Punkte thematisieren:

1. Ihre Einschätzung zum erforderlichen Stand der Technik gemäß § 3 Abs. 1 TTDSG zur Einhaltung des Fernmeldegeheimnisses;
2. Äußerungen von Sicherheitsexperten zur Thematik der Sicherheitsabfrage;
3. Ihre Einschätzung zur Eignung von Sicherheitsfragen auch bei niedrigem Vertrauensniveau.

Die Beantwortung Ihrer Punkte werde ich aus Verständnisgründen in umgekehrter Reihenfolge vornehmen.

Zu Punkt 3:
Für einen Dienst mit dem Vertrauensniveau „niedrig“ im Rahmen der Verwaltungsportale ist wesentlich, dass u.a. durch eine eventuelle Offenlegung der Daten „Keine Daten mit Personenbezug oder Daten, bei deren Offenlegung mit nur geringfügigen Auswirkungen für den Betroffenen zu rechnen ist.“[1] übermittelt werden. Diese Vorge-

[1] Siehe https://vn-check.ozg-umsetzung.de/

./.

Wagmüllerstraße 18
80538 München
Postfach 22 12 19
80502 München

Telefon: 089 212672-0
Telefax: 089 212672-50
https://www.datenschutz-bayern.de
poststelle@datenschutz-bayern.de

hensweise entspricht dem risikobasierten Ansatz der Datenschutz-Grundverordnung (DSGVO). Weitere Bedingungen entnehmen Sie bitte dem bereits im letzten Schreiben erwähnten OZG Praxistool Vertrauensniveau.

Ich möchte dies anhand von zwei Beispielen erläutern:

Angenommen ein(e) BürgerIn möchte ihre/seine eigenen Meldedaten abfragen. Diese Abfrage ist in Bayern online möglich; allerdings erfordert dies eine Authentifizierung mit eID, also z.B. mit dem Personalausweis. Der Service wird als Service mit einem höheren Vertrauensniveau als „niedrig" eingestuft.

Eine Meldung von Insektennestern hingegen kann i.d.R. bereits mit der Registrierungsart „Benutzername/Passwort" online abgegeben werden. Da hier lediglich eine Meldung und eine eventuelle Kontaktaufnahme für Rückfragen i.d.R. telefonisch und nicht über das BayernPortal erfolgt, kann das Vertrauensniveau als niedrig eingestuft werden. Die empfangende Behörde übermittelt zudem keine personenbezogenen Daten zurück an die/den BürgerIn.

Sowohl die Bewertung zur Notwendigkeit der Umsetzung des RFC 7672 DANE SMTP bzw. der BSI-Richtlinie TR 03108 wie auch der Einsatz von Sicherheitsabfragen erfolgt unter der einschränkenden Voraussetzung, dass es sich um Verwaltungsvorgänge mit dem Vertrauensniveau „niedrig" handelt. Die Gründe für diese Einschränkung entnehmen Sie meinem Schreiben vom 25. Juli 2022.

Zu Punkt 2:
In meinem letzten Schreiben teilte ich Ihnen bereits mit, dass ich hier für mich keinen Handlungsbedarf sehe. Wie Ihnen auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) mit seinen Schreiben vom 16. November 2021 und 25. Mai 2022 in Ihrer Anfrage #230874 bei fragdenstaat.de mitteilte, ist beim Vertrauensniveau „niedrig" mit den derzeit ergriffenen Maßnahmen kein Unterschreiten des zwingend notwendigen Stands der Technik gem. Art. 32 Datenschutz-Grundverordnung (DSGVO) erkennbar.

./.

Sicherlich bringen Sicherheitsabfragen per se einige Schwachstellen mit sich. Da sie allerdings nicht als alleinige Methode zur Informationspreisgabe eingesetzt werden, sondern die gewünschten Informationen per E-Mail an den Nutzer gesendet werden, müsste ein erfolgreicher Angriff sowohl den Zugriff auf die E-Mails (beim Transport oder durch Zugriff auf das jeweilige Postfach) wie auch die Beantwortung der Sicherheitsfrage umfassen.

Art. 32 DSGVO sieht keine festen Maßnahmenkataloge vor, sondern fordert eine Abwägung zwischen dem Stand der Technik, den Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos. Diese Abwägung wurde vom Verantwortlichen für das konkrete Szenario getroffen.

Da ich auch nach Ihren ergänzenden Darlegungen keine substantiierten Hinweise für ein Unterschreiten des notwendigen Sicherheitsniveaus für das vorliegende Szenario (Verwaltungsvorgang mit niedrigen Sicherheitsniveau) habe, habe ich weder Veranlassung noch aufsichtliche Handhabe gegen den Verantwortlichen, die Abschaffung der Sicherheitsfrage zu fordern.

Zu Punkt 1:
E-Mails, die aus dem BayernPortal verschickt werden, dienen ausschließlich der Benachrichtigung über neu eingegangene Nachrichten im Postfach der BayernID sowie der Unterstützung bei Registrierung und vergessenen Passwort.

Nach § 3 Abs. 2 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) unterliegen Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten der Pflicht zur Wahrung des Fernmeldegeheimnisses. Im Falle der gegenständlichen Vorgänge des automatisierten E-Mail-Versands (ohne Antwortmöglichkeit) durch ein Verwaltungsportal ist es zweifelhaft, ob hierin ein (selbständiger) Telekommunikationsdienst zu sehen ist.

Stellt man hingegen auf die Nutzung Ihres persönlichen E-Mail-Postfachs innerhalb des Verwaltungsportals ab, kann der Betreiber des Verwaltungsprotals nicht dessen Auslieferer sein.

Das Fernmeldegeheimnis ist für diese Vorgänge somit m.E. nicht einschlägig. Zudem würde das TTDSG auch keine gesetzliche Festlegung zu den erforderlichen technisch-organisatorischen Maßnahmen treffen.

Das StMGP hat aufgrund Ihrer Beschwerde bereits zugesagt, diese E-Mails zukünftig durch das Erzwingen von TLS (auch beim niedrigen Vertrauensniveau) abzusichern. Eine zwingende Notwendigkeit zur Umsetzung des RFC 7672 DANE SMTP bzw. der BSI-Richtlinie TR 03108 sehe ich aus diesem Grund hier nicht, auch wenn dies natürlich aus der Sicht der IT-Sicherheit wünschenswert wäre. Ich habe daher auch hier keine Veranlassung und Möglichkeit, weitere aufsichtliche Maßnahmen zu ergreifen.

Ich betrachte mit diesem Schreiben den Vorgang Ihrer Beschwerde als abgeschlossen. Ich weise bereits vorsorglich darauf hin, dass gem. § 17 Abs. 3 Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern entsprechend gleichartige Eingänge ohne **neuen Tatsachenvortrag oder neue Gesichtspunkte**, nicht mehr beantwortet werden. Sollten neue Aspekte ohne Darlegung der persönlichen Betroffenheit eingehen, werde ich diese unbeantwortet als Prüfungsanregung aufnehmen.

Mit freundlichen Grüßen

[redacted]