BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

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

Joachim Lindenberg
Heubergstraße 1a
76228 Karlsruhe

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-[redacted]
E-MAIL Referat16@bfdi.bund.de
BEARBEITET VON [redacted]
INTERNET www.bfdi.bund.de
DATUM Bonn, 24.05.2023
GESCHÄFTSZ. 16-206 II#1228

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

BETREFF **Datenschutzaufsichtsbehördliches Verfahren**
HIER Anhörung nach § 28 Verwaltungsverfahrensgesetz (VwVfG)
BEZUG Ihre Beschwerde vom 3. Oktober 2021; erste Anhörung vom 19. Mai 2023

ANHÖRUNG

Sehr geehrter Herr Lindenberg,

ich beabsichtige Ihre Beschwerde vom 3. Oktober 2022 gegen das Bundesministerium des Innern und für Heimat (BMI) gemäß Art. 77 Abs. 2 Datenschutz-Grundverordnung (DSGVO) abzuweisen.

Begründung:

I.

Mit E-Mail vom 3. Oktober 2021 erhoben Sie eine datenschutzrechtliche Beschwerde, wobei sie in Ihren weiteren E-Mails vom 9. und 11. Oktober 2021 konkretisiert haben, dass Sie diese gegen das BMI richten. Nach meinem ersten Anhörungsschreiben vom 19. Mai 2023 haben Sie in Ihrer weiteren E-Mail vom 21. Mai 2022 weiter vorgetragen.

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

Sie haben ein Nutzerkonto beim BMI, welches Teil der Maßnahme „bund ID“ ist. Der Betrieb des Nutzerkontos Bund erfolgt im Auftrag des verantwortlichen BMI durch das Informationstechnikzentrum Bund (ITZBund) als Auftragsverarbeiter. Für das BMI liegt keine formale Zertifizierung nach ISO 27001 auf Basis des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vor. Das ITZBund ist hingegen als Betreiber des Nutzerkontos nach IT-Grundschutz ausgerichtet. Die Maßnahme „bund ID“ befindet sich zudem in einem strukturierten, kontinuierlichen Verbesserungsprozess gemeinsam mit dem BSI. Im Zuge dessen wird eine Zertifizierung des Informationsmanagementsystems nach ISO 27001 auf Basis IT-Grundschutz angestrebt. Auch werden jährliche IS-Pentests und IS-Webchecks durchgeführt. Das Schutzniveau wird regelmäßig im Rahmen einer Schutzbedarfsfeststellung durch das BMI geprüft und aktualisiert. Diese Aktualisierung fließt in den kontinuierlichen Verbesserungsprozess der IT-Sicherheitskonzeption ein.

Es gelten insbesondere folgende Anforderungen nach IT-Grundschutz-Kompendium:

- Gemäß *IT-Grundschutz-Kompendium (Edition 2021, NET.1.1.A7)* müssen schützenswerte Informationen über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, sofern nicht über vertrauenswürdige dedizierte Netzsegmente (z. B. innerhalb des Managementnetzes) kommuniziert wird. Können solche Protokolle nicht genutzt werden, muss nach dem Stand der Technik angemessen verschlüsselt und zu authentisiert werden (siehe NET.3.3 VPN).

- Ferner wird lt. *IT-Grundschutz-Kompendium (Edition 2021, SYS.1.8.A23)* empfohlen, alle in Speicherlösungen abgelegten Daten zu verschlüsseln und festzulegen, auf welchen Ebenen (Data-in-Motion und Data-at-Rest) verschlüsselt wird. Dabei wird darauf hingewiesen, dass die Verschlüsselung auf dem Transportweg auch bei Replikationen und Backup-Traffic relevant ist. Dies wurde im Rahmen der Risikoanalyse nach IT-Grundschutz Methode berücksichtigt.

Sie behaupten, dass Verschlüsselung nicht oder nicht konsequent umgesetzt sei, insbesondere NET.1.1.A7 und SYS 1.8 A23. Sie vertreten daher die Ansicht, dass das BMI kein der DSGVO angemessenes Schutzniveau für die Verarbeitung personenbezogener Daten erfülle. Sie stellen in Frage, dass in Speicherlösungen verschlüsselt werde, und bitten mich

um Klärung, ob tatsächlich verschlüsselt wird. Zudem machen Sie allgemeine Ausführungen zu Grundschutz, Bedrohungsanalysen und Zertifizierungen.

Das BMI behauptet und hat gegenüber mir dargelegt, dass der Schutzbedarf bezüglich der Vertraulichkeit aktuell als „hoch" eingestuft sei und in der Anwendung der IT-Grundschutzmethode zur Absicherung der Maßnahme „bund ID" entsprechend berücksichtigt werde. Die Absicherung der Maßnahme bund ID entspreche den Vorgaben und erfolge auf Basis des IT-Grundschutzes. Dies schließe die verpflichtende Basis-Anforderung NET.1.1.A7 mit ein. Sowohl die interne als auch die externe Kommunikation der Maßnahme bund ID sei hiervon betroffen. Die Maßnahme bund ID nutze standardmäßig TLS-Verschlüsselung. Die Absicherung für die bund ID erfolgt auf Basis von IT-Grundschutz, wobei das BMI auch auf IT-Grundschutz-Kompendium (Edition 2021, SYS.1.8.A23) verweist. Das BMI teilt somit Ihre Ansicht nicht, dass kein angemessenes Schutzniveau im Kontext DSGVO für die Verarbeitung personenbezogener Daten erfüllt sei.

Das BMI hat nunmehr ausdrücklich ergänzend vorgetragen, dass die Speicherlösung verschlüsselt ist und die Sicherheitskonzeption, insbesondere die Risikoanalyse, regelmäßig unter Einbeziehung des BSI überprüft wird.

II.

Gemäß § 9 Abs. 1 S. 1 Bundesdatenschutzgesetz (BDSG) ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) für die Datenschutzaufsicht über das BMI zuständig.

Nach Art. 77 DSGVO hat jede betroffene Person das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt. Gemäß Art. 57 Abs. 1 lit. f) DSGVO habe ich im Rahmen meiner Untersuchung zu Ihrem Beschwerdefall nach den bisherigen Sachverhaltsfeststellungen keinen datenschutzrechtlichen Verstoß feststellen können.

Ein Datenschutzverstoß seitens des BMI liegt nicht vor.

Das BMI hat dargelegt, dass bei der Verarbeitung personenbezogener Daten beim Betrieb von BMI-Nutzerkonten, welche Teil der Maßnahme „bund ID" sind, Verschlüsselungstechniken eingesetzt werden. Diese entsprechen den Vorgaben des BSI.

Dabei handelt es sich um geeignete technische und organisatorische Maßnahmen, die im Sinne von Art. 32 Abs. 1 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dass das BMI selbst nicht nach BSI-Grundschutz zertifiziert ist, ist unschädlich. Eine solche technische Zertifizierung des Verantwortlichen oder des Auftragsverarbeiters ist nach DSGVO nicht zwingend erforderlich. Gleichwohl indiziert die Ausrichtung des Auftragsverarbeiters ITZBund am IT-Grundschutz des BSI sowie die regelmäßigen Überprüfungen durch das BSI die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen.

III.

Bevor ich in der Sache eine endgültige Entscheidung treffe, gebe ich Ihnen bis zum

19. Juni 2023

gemäß § 28 VwVfG Gelegenheit, sich zur Sache zu äußern.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Beglaubigt

[redacted]