Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

Nur elektronisch:

c.franke.6.gu36kykksw@fragdenstaat.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-[redacted]
E-MAIL referat11@bfdi.bund.de
BEARBEITET VON [redacted]
INTERNET www.bfdi.bund.de
DATUM Bonn, 16.11.2021
GESCHÄFTSZ. 11-103 II#7156

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

BETREFF **Ihre Anfrage beim BfDI über FragdenStaat**
HIER Verschlüsselung und Sicherheit der Verwaltungsportale

Sehr geehrte Frau Franke,

vielen Dank für Ihre Eingabe beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). In Ihrer Eingabe bewerten Sie einige technische Entscheidungen bei der Ausgestaltung des Nutzerkontos Bund (NKB) kritisch und fragen, ob diese Ausgestaltung mit den Anforderungen der DSGVO und des BDSG vereinbar sei. Insbesondere kritisieren Sie die Nutzung (vorformulierter) Sicherheitsfragen als Teil des Authentifizierungskonzeptes, den Rückgriff auf eine andere Domain beim Versenden von E-Mails als bei der Anmeldung ins NKB selbst sowie die nichtoptionale Ausgestaltung der Postfacheinrichtung. Daneben erwähnten Sie noch die Benennung der Rechtsgrundlagen in der Datenschutzerklärung des NKB.

Weiterhin kritisieren Sie einige technische und rechtliche Entscheidungen bei der Einrichtung diverser Nutzerkonten der Länder. Hier will ich allerdings vorab darauf hinweisen, dass ich insofern nicht für Ihre Anliegen zuständig bin, sondern allein die jeweiligen Datenschutzaufsichtsbehörden der Länder. Dem BfDI liegen hierzu ohnehin keine belastbaren eigenen Erkenntnisse vor.

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

Zu Ihren Kritikpunkten:

1. (Vorformulierte) Sicherheitsfragen

Es ist zutreffend, dass auch das NKB vorformulierte Sicherheitsfragen verwendet. Nach Ansicht des BfDI handelt es sich dabei jedoch nicht um ein Unterschreiten des gemäß Art. 32 DSGVO für die Verarbeitung personenbezogener Daten zwingend notwendigen Stands der Technik. Der Stand der Technik ist kein einheitlicher Anforderungskatalog, sondern bemisst sich nach dem jeweiligen Verarbeitungsszenario. Verarbeitungsszenario ist hier allein eine Hilfsfunktion im ohnehin niedrigsten Vertrauensniveau des NKB. Da schon zum Anlegen dieser (im niedrigsten Vertrauensniveau angesiedelten) Basisregistrierung allein der Zugang zum E-Mail-Account ausreicht und dort dem Stand der Technik entspricht, gilt dies auch für die ähnlich konstruierte Sicherheitsfrage, die damit verknüpft ist. Ein zusätzliches Sicherheitsmerkmal darüber hinaus würde die Anforderungen an das niedrigste(!) Vertrauensniveau bereits verlassen und in höhere Sphären vordringen.

2. Domainabweichung

Es ist zutreffend, dass auch das NKB beim Versenden von E-Mails auf eine andere Domain zurückgreift, als die Anmeldung beim NKB selbst. Nach Ansicht des BfDI handelt es sich dabei jedoch nicht um ein Unterschreiten des Stands der Technik im Sinne des Art. 32 DSGVO. Die Abweichung findet allein auf der Third-Level-Domain statt (Anmeldebestätigung: bmi.bund.de vs. NKB-Anmeldung: id.bund.de). Ein Sicherheitsrisiko, dass den Stand der Technik unterschreitet, ist bei gleichbleibender Second-Level-Domain nicht erkennbar / etabliert.

3. Postfach im NKB

Es ist zutreffend, dass das Postfach des NKB sofort nach der Registrierung vorhanden ist. Nach Ansicht des BfDI handelt es dabei ebenfalls nicht um ein Unterschreiten des Stands der Technik im Sinne des Art. 32 DSGVO. Vielmehr stellt dies ein übliches Verhalten dar bei solchen Systemen. Auch steht diese Eigenschaft nicht im Widerspruch zu den rechtlichen Anforderungen gemäß § 2 Abs. 7 OZG. Danach ist das Postfach Bestandteil des Nutzerkontos, aber die Nutzung dessen ist freiwillig. Die gesetzliche Regelung sieht die Einrichtung des Postfachs an sich also gerade als unabhängig vom eigentlichen Nutzungswillen an.

4. Datenschutzerklärung des NKB

Es ist zutreffend, dass sich das NKB in seiner Datenschutzerklärung auf Art. 6 Abs. 1 lit. e) DSGVO in Verbindung mit den jeweils hauptsächlich einschlägigen Normen des OZG selbst beruft. Nach Ansicht des BfDI ist dieses Vorgehen korrekt und kein Verstoß gegen Art. 13, 14 DSGVO. Art. 6 Abs. 1 lit. e) DSGVO dient der Rechtfertigung der Verarbeitung personenbezogener Daten für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Allgemein wird diese Variante als einschlägig angesehen für die Verarbeitung insbesondere durch öffentliche Stellen in Erfüllung ihres gesetzlichen Auftrags. Der Bund / Das BMI haben durch die (ebenfalls mitzitierten) Regelungen des OZG den gesetzlichen Auftrag ein Nutzerkonto zu betreiben. Jedwede Datenverarbeitungen, die also hierfür notwendig sind, sind gleichzeitig notwendig für die Erfüllung des gesetzlichen Auftrags und können so über Art. 6 Abs. 1 lit. e) DSGVO rechtfertigt werden.

Ihre Vermutung, dass Art. 6 Abs. 1 lit. c) DSGVO einschlägig sein sollte, ist insofern unzutreffend. Gemäß Art. 6 Abs. 1 lit. c) DSGVO sind Verarbeitungen auch dann rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich sind, die der Verantwortliche unterliegt. Zielrichtung dieses Rechtfertigungsgrunds ist aber weniger der Staat selbst, sondern eher private Verantwortliche, die von einer staatlichen Auflage betroffen sind (ein zeitgerechtes Beispiel wäre wohl das Anfertigen von Gästelisten beim Zugang zu einem Restaurant o. ä. durch den Betreiber, weil eine Coronaschutzverordnung des jeweiligen Landes dies zwingend vorschreibt).

Wie von Ihnen zutreffend angemerkt, sollte die Rechtsgrundlage der Einwilligung gemäß Art. 6 Abs. 1 lit. a) DSGVO bei den eigentlichen Hauptleistungen des Nutzerkontos keine Rolle spielen.

Ich hoffe, dass ich Ihnen damit weiterhelfen konnte. Sollten Sie noch Fragen in der Sache haben, können Sie sich gerne wieder an mich wenden.

Mit freundlichen Grüßen
Im Auftrag

[redacted]