BfDI

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

BfDI | Postfach 1468 | 53004 Bonn

Joachim Lindenberg
Heubergstr. 1a
76228 Karlsruhe

Ihr Kontakt:
[redacted]
Telefon: +49 228 997799
[redacted]
E-Mail:
Referat15@bfdi.bund.
de

Aktenz.: 15-302 II#2441
(bitte immer angeben)
Dok.: 100006/2024

Anlage:

Bonn, 17.04.2025

Datenschutzaufsichtsbehördliches Verfahren
Ihre Beschwerden vom 29.11.2023 und 21.05.2024

A N H Ö R U N G

Sehr geehrter Herr Lindenberg,

ich beabsichtige Ihrer Beschwerde vom 29.11.2023 und 21.05.2024 gegen die Bundesagentur für Arbeit (BA) gemäß Art. 77 Abs. 2 Datenschutz-Grundverordnung (DSGVO)

1a. stattzugeben, soweit diese die nicht fristgerechte Beantwortung Ihres nach Art. 15 Abs. 1 und 3 DSGVO beantragten Auskunftsersuchens vom

04.10.2023 innerhalb der nach Art. 12 Abs. 3 DSGVO normierten Monatsfrist betrifft.

1b. die Beschwerde abzuweisen, soweit diese eine unvollständige Auskunft bei Erteilung der Auskunft am 15.10.2024 betrifft.

2. die Beschwerde abzuweisen, soweit diese einen Anspruch auf einen E-Mail-Versand durch die BA mittels qualifizierter Transportverschlüsselung mit dem DNSSEC/DANE Sicherheitsstandard fordert.

3. die Beschwerde abzuweisen, soweit ein Verstoß gegen Art. 13 DSGVO durch den Einsatz des USB-Sticks der BA vorgebracht wurde und dass die Auskunft nach Art 12. Abs. 3 S. 4 DSGVO nicht in einem gängigen elektronischen Format erfolgte.

4. die Beschwerde abzuweisen, soweit Verstöße gegen Art. 32 DSGVO vorgebracht wurden, da das Passwort des USBs unsicher sei und der USB-Stick und das Passwort postalisch übermittelt wurden.

Begründung:

I.

Sie sind für Ihre Tochter kindergeldberechtigt. Im Rahmen der Erbringung des Kindergeldes werden ihre personenbezogene Daten bei der Familienkasse Baden-Württemberg West der BA verarbeitet.

Außerdem hatten Sie sich zuvor wegen verschiedener Anliegen an die Pressestelle und Stabsstelle Datenschutz der BA gewandt. Im Leistungsbezug bei einer Agentur für Arbeit befinden Sie sich jedoch nicht.

Zu 1.)

Am 04.10.2023 stellten Sie einen Auskunftsantrag nach Art. 15 Abs. 1 und 3 DSGVO über das Kontaktformular der BA. Es erfolgte eine Auskunft durch die o.g. Familienkasse, die in einem separaten Beschwerdeverfahren bei der BfDI bearbeitet wird.

a) Von der Agentur für Arbeit Karlsruhe-Raststatt erhielten Sie eine schriftliche Negativauskunft (es werden keine Daten verarbeitet) mit Schreiben vom 07.11.2023. Zu diesem Zeitpunkt erhielten Sie jedoch keine Auskunft bezüglich der Verarbeitung Ihrer Daten durch die Pressestelle der BA und die Stabsstelle Datenschutz der BA. Mit Schreiben vom 29.11.2023 erhoben Sie diesbezüglich eine datenschutzrechtliche

Beschwerde gegen die BA. Infolge Ihrer Beschwerde erteilte Ihnen die BA mit Schreiben vom 15.05.2024 elektronisch Auskunft, die Ihre gespeicherten personenbezogenen Daten bei der Pressestelle und Stabsstelle Datenschutz der BA umfasste. Vorausgegangen war eine separate, postalische Auskunft der Pressestelle ohne Daten der Stabsstelle Datenschutz.

b) Mit Schreiben vom 21.05.2024 an die BA und an mich monierten Sie eine nicht vollständig erfolgte Auskunftserteilung, da Angaben nach Art 15 Abs. 1 DSGVO, die interne Kommunikation zwischen den Stellen der BA, fehle und die zuvor nicht zentral erfolgte Auskunft der BA. Die BA beteuert, dass solche Kommunikationen nicht vorliegen würden und die Auskunft vollständig erfolgt sei.

Zu 2.)

Per E-Mail nahmen Sie am 10.11.2023 Kontakt mit dem Ansprechpartner für Datenschutzangelegenheiten der Agentur für Arbeit Karlsruhe-Rastatt auf, der Ihnen mit einer E-Mail vom 13.11.2023 antwortete, dass die Agentur für Arbeit für Ihr Auskunftsersuchen unzuständig sei. Da keine qualifzierte Transportverschlüsselung mit dem Sicherheitsstandard DNSSEC/DANE verwendet wurde, sehen Sie in dem E-Mail-Versand einen Datenschutzverstoß. Die BA räumt einen Datenschutzverstoß insoweit ein, dass der Mitarbeiter gegen die interne Weisung der BA verstoßen habe, keine nicht Ende-zu-Ende verschlüsselten E-Mails mit Sozialdaten an Kunden zu versenden.

Zu 3.)

Die Auskunft vom 15.05.2024 wurde mittels zwei Schreiben auf dem Postweg erteilt: Das erste Schreiben enthielt den USB-Stick des Modells „Kanguru Defender Elite 300“ ,der die Auskünfte gespeichert enthielt. Der USB-Stick kann zudem optional zentral verwaltet werden und somit können die Daten beispielsweise per Fernzugriff gelöscht werden. Laut Angabe der BA verwendet sie eine speziell angepasste Firmwareversion: Funktionen, wie die Verwendung eines Masterpassworts, der Remotezugriff, herstellerspezifische Antivirus-Software, Cloudanbindung sowie eine Logging-Möglichkeit sind in der BA-sind in der BA-Firmewareversion nicht enthalten. Aufgrund der zentralen Verwaltbarkeit des USB-Stickes sind Sie der Auffassung, dass ein Hinweis oder eine Angabe in der Datenschutzerklärung zu der Funktion enthalten hätte sein müssen, ob diese Funktion genutzt wird oder nicht, und falls ja, wer den

Dienst dazu verantwortet oder betreibe. Die Auskunft erfolge zudem mit diesem USB-Stick auch nicht in einem gängigen elektronischen Format.

Zu 4.)

Das zweite Schreiben der BA enthielt ein Passwort für den USB-Stick. Das Passwort bestand aus elf Zeichen, Klein- und Großbuchstaben, Sonderzeichen und Zahlen. Die Reihenfolge der Zeichen entsprechen einem Muster, mit der Abkürzung „Ae“ für Auskunftserteilung, den Initialien Ihres Vor- und Nachnamens und des Datums (TTMMJJ) des Auskunftsschreibens. Nach zehn Fehlversuchen der Passworteingabe werden die Daten auf dem USB-Stick gelöscht. Mit Schreiben vom 21.05.2024 an die BA und mich monieren Sie die Übermittlung des USB-Sticks und des Passworts auf postalischen Wege sowie die mangelhafte Sicherheit des Passworts.

II.

Gemäß § 9 Abs. 1 Bundesdatenschutzgesetz (BDSG) ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) für die Datenschutzaufsicht über die öffentlichen Stellen des Bundes zuständig. Die BA ist eine öffentliche Stelle des Bundes, § 367 Abs. 1 Drittes Buch Sozialgesetzbuch (SGB III).

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 folgende Ergebnisse festgestellt:

Zu 1.)

Für betroffene Personen besteht das Recht, einen Antrag auf Auskunft über die beim Verantwortlichen verarbeiteten personenbezogenen Daten gemäß Art. 15 DSGVO zu stellen. Die verantwortliche Stelle hat die Auskunft gemäß Art. 12 Abs. 3 S. 1 DSGVO grundsätzlich unverzüglich, spätestens jedoch innerhalb eines Monats nach Antragstellung zu erteilen. Zu dem Recht auf Auskunft gehören nach Art. 15 Abs. 3 DSGVO der Erhalt einer Kopie der personenbezogenen Daten. Nach Art. 12 Abs. 3 S. 4 DSGVO hat die Auskunft in elektronischer Form in einem gängigen Format zu erfolgen, wenn der Betroffene den Antrag elektronisch stellt. Nach der

von Ihnen angeführten Leitlinie 01/2022 des Europäischen Datenschutzausschusses zum Auskunftsrecht Version 2.1 vom 28. März 2023, Randnummer 136 sollen Verantwortliche, die große Datenmengen verarbeiten, die Daten aus mehreren Abteilungen zusammengefasst mitteilen.

Zu 1a) Die BA hatte Ihnen zunächst eine nicht zutreffende Negativauskunft erteilt. Nach Einlegung Ihrer Beschwerde wurden Ihnen dann zunächst eine nicht-elektronische Teilauskunft durch die Pressestelle der BA erteilt. Erst mit Übersendung des USB-Sticks mit Schreiben vom 15.05.2024 wurde Ihnen zentral die Gesamtauskunft auf elektronischem Wege erteilt. Dies lag weit außerhalb der Frist des Art. 12 Abs. 3 DSGVO und es liegt daher ein Datenschutzverstoß vor. Ihrer Beschwerde wird in diesem Punkt stattgegeben. Von einer Maßnahme nach Art. 58 Abs. 2 DSGVO sehe ich aus Gründen der Verhältnismäßigkeit ab, da es sich um einen besonderen Einzelfall handelt, die BA die Auskunft letztendlich erteilt und sich kooperativ gezeigt hat. Zur Optimierung des Verfahrens der Auskunftserteilung steht die BfDI im Übrigen in einem Beratungsprozess mit der BA.

Zu 1b) Die BA hat mir nachvollziehbar dargelegt, dass Sie von der Pressestelle und der Stabsstelle Datenschutz eine Auskunft über alle gespeicherten personenbezogenen Daten erhalten haben. Daher gehe ich davon aus, dass Ihnen die Auskunft mit Schreiben vom 15.05.2024 vollständig erteilt wurde. Ihre Beschwerde wird hinsichtlich der unvollständigen Auskunftserteilung abgewiesen.

Zu 2.) Art. 32 DSGVO verpflichtet Verantwortliche geeignete technische und organisatorische Maßnahmen (TOM) zu ergreifen, um ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten. Dabei sind insbesondere die Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen, einschließlich der Risiken durch unbefugte Offenlegung oder Zugang zu personenbezogenen Daten.

Die BfDI teilt die Ausführungen der „Orientierungshilfe zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail" der DSK vom 27. Mai 2021. Demnach sind Verantwortliche und Auftragsverarbeiter gesetzlich gehalten, die Risiken, die sich aus Verarbeitungen personenbezogener Daten ergeben, hinreichend zu mindern. Sie müssen hierbei Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen

berücksichtigen. Beim E-Mail-Versand sind mögliche Verschlüsselungswege die Transportverschlüsselung und die Ende-zu-Ende-Verschlüsselung. Bei Sozialdaten handelt es sich um besonders sensible Daten. Nach Auffassung der BfDI sollte beim Versand von Sozialdaten generell von einem hohen Risiko ausgegangen werden und somit nur Ende-zu-Ende verschlüsselt übermittelt werden. Die BA teilt diese Auffassung und hat eine entsprechende Weisung erlassen.

Der Versand der E-Mail mit Sozialdaten vom 13.11.2023 durch die BA fand dennoch ohne eine Ende-zu-Ende Verschlüsselung statt. Demnach liegt ein Verstoß gegen Art. 32 DSGVO vor. Ihrer Beschwerde wird daher in diesem Punkt stattgegeben. Von einer aufsichtsrechtlichen Maßnahme sehe ich aus Gründen der Verhältnismäßigkeit ab, da die BA bereits eine Weisung zwecks verschlüsselter Kommunikation via E-Mail erlassen hat. Es handelt sich nicht um ein strukturelles Problem, sondern vorliegend hat ein Mitarbeiter im Einzelfall dagegen verstoßen. Seitens der BA wurde zudem bereits datenschutzrechtlich sensibilisiert.

Einen Anspruch hieraus, dass die BA flankierend zur Transportverschlüsselung den Sicherheitsstandard DNSSEC/DANE einsetzen muss leitet sich aus Art. 32 DSGVO jedoch nicht ab. Ihre Beschwerde wird in diesem Punkt daher abgewiesen.

Zu 3.) Nach Art. 13 DSGVO muss der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung personenbezogener Daten u.a. mitteilen, für welche die Zwecke die personenbezogenen Daten verarbeitet werden sollen (lit. c) und die Empfänger (lit. e) der personenbezogenen Daten mitteilen. Weitergehende Informationspflichten, ob bestimmte Funktionen aktiviert sind oder nicht, sind datenschutzrechtlich nicht normiert.

Im Gegensatz zu den ursprünglichen Funktionsmöglichkeiten des USB-Sticks nutzt die BA eine angepasste Firmware, die keine personenbezogenen Daten übermittelt oder zu einem anderen Zweck als der Speicherung nutzt. Es liegt daher keine Erforderlichkeit einer Informationspflicht diesbezüglich nach Art. 13 DSGVO vor.

Stellt die betroffene Person ihr Auskunftsersuchen elektronisch, sind die Informationen nach Art. 12 Abs. 3 S. 4 DSGVO und Art. 15 Abs. 3 S. 3 DSGVO – sofern die betroffene Person nichts Anderes angibt – in einem gängigen elektronischen Format zur Verfügung zu stellen. Ein „gängiges elektronisches Format“ ist beispielsweise das PDF-Format. Das Format hat keinen Einfluss auf das Medium (USB-Stick), auf dem die Auskunft erteilt

wird und es liegt kein Verstoß gegen Art. 12 Abs. 3 S. 4 DSGVO vor. Ihre Beschwerde wird daher in diesem Punkt abgewiesen.

Zu 4.) Bei der Erteilung der elektronischen Auskunft ist darauf zu achten, dass bestimmte Datensicherheitsmaßnahmen getroffen werden. Art. 32 DSGVO ist entsprechend anzuwenden.

Vorgaben zu Sicherheitsstandards für Passwörter erfolgen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Nach den Hinweisen des BSI[1] sollte ein kurzes und komplexes Passwort mindestens acht Zeichen lang sein und aus vier verschiedenen Zeichenarten (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) bestehen. Diese Kriterien sind bei dem von der BA erstellten Passwort überwiegend voll berücksichtigt. Das Passwort folgt einem Muster anstatt einer willkürlichen Reihenfolge der Zeichenarten. Die Passwort-Entropie ist durch die Verwendung des Musters niedriger. Nach Eingabe von 10 Fehlversuchen werden die Daten auf dem USB-Stick unwiderruflich gelöscht. Im Rahmen einer Gesamtabwägung halte ich das verwendete Passwort in Kombination mit diesem Sicherheitsmechanismus als getroffene Datensicherheitsmaßnahme für ausreichend. Ein Verstoß gegen Art. 32 DSGVO liegt daher nicht vor.

Der getrennte Versand von geschützten Unterlagen ist eine anerkannte technisch-organisatorische Maßnahme, um personenbezogene Daten zu schützen. Beim Versand von Authentifizierungsinformationen sollte darauf geachtet werden, dass die Informationen getrennt übermittelt werden, um das Risiko eines unbefugten Zugriffs zu minimieren. Die Methode des getrennten Versands per Post ist ein Best Practice zur Sicherheit sensibler Daten und wird auch von Banken und Finanzbehörden eingesetzt. Einen gesetzlichen Anspruch darauf, diese auf unterschiedlichen Kommunikationswegen zu übersenden gibt es nicht.

Ihre Beschwerde wird daher in diesem Punkt abgewiesen.

III.

---

1 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=4

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

20. Mai 2025

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

Mit freundlichen Grüßen
Im Auftrag

[redacted]

[redacted]