Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117
FON (0228) 997799-1555
E-MAIL Referat15@bfdi.bund.de
BEARBEITET VON Herr Dr. Kisker
INTERNET www.bfdi.bund.de

DATUM Bonn, 14.12.2023
GESCHÄFTSZ. 15-302-2/381#3282

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

An die Geschäftsführungen der Jobcenter

nachrichtlich:
Stabsstelle Datenschutz der Bundesagentur für Arbeit

Bundesministerium für Arbeit und Soziales
Referat IIa1
Referat IIc1

BETREFF **Rundschreiben Nummer 11**
BEZUG Runder Tisch vom 13. und 14. September

Sehr geehrte Damen und Herren,

mit diesem Rundschreiben möchte ich die Inhalte und Ergebnisse des zweiten Runden Tischs zum Datenschutz in der Arbeitsverwaltung aufbereiten und allen behördlichen Datenschutzbeauftragten der Jobcenter, auch denen, die am Runden Tisch nicht persönlich teilnehmen konnten, zur Verfügung stellen. Darüber hinaus erfolgt eine Klarstellung zum Bericht über den letzten Runden Tisch.

Im Hause des BfDI in Bonn trafen sich je ein behördlicher Datenschutzbeauftragter/eine behördliche Datenschutzbeauftragte eines Jobcenters eines Bundeslandes mit Vertreterinnen und Vertretern der Bundesagentur für Arbeit, des Bundesministeriums für Arbeit und Soziales sowie Mitarbeiterinnen und Mitarbeitern des BfDI.

Die Veranstaltung diente, wie im letzten Jahr, neben dem direkten Austausch über alle Beteiligte betreffende aktuelle Themen des Datenschutzes in der Arbeitsverwaltung, dem Vernetzen der Beteiligten untereinander und dem persönlichen Austausch. Auch dieses Jahr wurden diese Ziele nach meinem Eindruck und den Rückmeldungen, die uns erreicht haben,

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 E
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenminist

voll erreicht – insbesondere der Ablauf als zweitägige Veranstaltung wurde von allen Seiten als gelungen wahrgenommen.

Wir möchten uns bei allen Teilnehmerinnen und Teilnehmern für den teils kontroversen, aber stets sachlichen Austausch und Ihre rege Mitwirkung bedanken.

I. Bericht zum Runden Tisch 2023:

TOP 1: Verfahren bei Meldungen nach Art. 33 DSGVO

Seitens des BfDI besteht die Wahrnehmung, dass sich die Verantwortlichen ihrer Verpflichtung zur Meldung von Datenschutzvorfällen nach Art. 33 DSGVO bewusst sind; jedoch besteht in der Meldepraxis Verbesserungsbedarf und es scheint Unsicherheit zu bestehen, wann überhaupt eine Datenschutzverletzung zu melden und wann die Betroffenen zu benachrichtigen sind. Mit den folgenden Ausführungen möchten wir Ihnen diesbezüglich eine Orientierungshilfe geben:

I. Sinn und Zweck

Datenschutzvorfälle sind häufig mit Risiken für Betroffene verbunden. Oft sind eine schnelle Aufklärung und das Ergreifen von Maßnahmen notwendig, die das Risiko verringern und den Betroffenen helfen, sich vor möglichen Schäden zu schützen. Aus diesem Grund sind Verantwortliche nach Art. 33 DSGVO grundsätzlich verpflichtet, eine Verletzung des Schutzes personenbezogener Daten (sog. Datenpannen oder Datenschutzvorfälle) an die zuständige Datenschutzaufsichtsbehörde zu melden und u. U. gem. Art. 34 auch verpflichtet, Betroffene zu benachrichtigen. Durch die zügige Meldung an die Datenschutzaufsichtsbehörde soll diese in die Lage versetzt werden, über Maßnahmen zur Eindämmung und ggfs. auch Ahndung der Rechtsverletzung zu entscheiden.

II. Grundvoraussetzung: Verletzung des Schutzes personenbezogener Daten

Anknüpfungspunkt für die Meldepflicht nach Art. 33 DSGVO und die Benachrichtigungspflicht nach Art. 34 DSGVO ist eine „Verletzung des Schut-

zes personenbezogener Daten“. Der Terminus ist in Art. 4 Nr. 12 DSGVO definiert.

Demnach liegt eine solche Verletzung nicht in jedem Verstoß gegen datenschutzrechtliche Vorschriften, sie bezieht sich vielmehr gerade auf eine Verletzung der Datensicherheit. Die Datensicherheit beinhaltet zum einen den Integritäts- bzw. Verfügbarkeitsschutz und umfasst die Vernichtung, den Verlust oder die Veränderung der personenbezogenen Daten. Zum anderen ist die unberechtigte Kenntnisnahme personenbezogener Daten, also der Vertraulichkeitsschutz, betroffen. In Zweifelsfällen ist der Begriff der Datensicherheit weit auszulegen.

III. Pflicht zur Meldung und zur Benachrichtigung

Bei der Frage, ob ein Datenschutzvorfall zu melden ist oder nicht, ist eine einzelfallbezogene Risikobeurteilung entscheidend: Prüfungsgegenstand ist im Fall von Art. 33 Abs. 1 DSGVO, ob ein Risiko für die Rechte und Freiheiten von Betroffenen als voraussichtliche Folge der Datenschutzverletzung ausgeschlossen werden kann. Ist dies der Fall, kann ausnahmsweise eine Meldung an den BfDI unterbleiben. Eine solche einzelfallbezogene Risikobeurteilung ist auch für das Vorliegen einer Benachrichtigungspflicht nach Art. 34 Abs. 1 DSGVO entscheidend: Ist der Vorfall voraussichtlich sogar mit einem hohen Risiko für Betroffene verbunden, hat der Verantwortliche zusätzlich diese zu benachrichtigen.

Einzelheiten der hier zu treffenden Risikoabwägung finden Sie in der anliegenden Folie.

IV. Frist für die Meldung und für die Benachrichtigung

Art. 33 DSGVO sieht eine Meldepflicht unverzüglich, möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung vor. Ein Bekanntwerden liegt vor, wenn dem Verantwortlichen über einen Datenschutzverstoß alle relevanten Tatsachen bekannt sind und er mit hinreichender Wahrscheinlichkeit die Rechtswidrigkeit im Hinblick auf die DSGVO erkennen kann. Dabei reicht es aus, dass nach einer vernünftigen Einschätzung ein Datenschutzverstoß nicht ausgeschlossen werden kann.

Insbesondere bei größeren und komplexeren Datenschutzvorfällen werden Verantwortliche u. U. länger als 72 Stunden benötigen, um alle Informationen zumutbar ermitteln zu können. Können daher noch nicht alle Informationen auf einmal bereitgestellt werden, sollte der Verantwortliche die Informationen auch schrittweise in Form einer vorläufigen Meldung dem BfDI zur Verfügung stellen. Bei der schrittweisen Zurverfügungstellung darf es jedoch nicht zu einer unangemessenen weiteren Verzögerung kommen.

Zudem hat der Verantwortliche auch die betroffenen Personen unverzüglich zu benachrichtigen, wenn der Vorfall voraussichtlich ein hohes Risiko für diese zur Folge hat (Art. 34 DSGVO).

V. Inhalt der Meldung

Die Meldung muss mindestens die inhaltlichen Angaben nach Art. 33 Abs. 3 DSGVO enthalten. Insbesondere erforderlich sind somit:

- Alle Fakten zum Verständnis, was genau passiert ist
  In der Meldepraxis wird der Sachverhalt hingegen oftmals nur rudimentär bzw. für „Außenstehende“, die nicht mit allen internen Prozessen der BA oder der Jobcenter vertraut sind, nicht nachvollziehbar beschrieben.

- Alle Fakten für die Nachvollziehbarkeit der Risikobewertung des Verantwortlichen
  In der Meldepraxis werden hier meist zu wenig Informationen mitgeteilt, damit der BfDI die getroffene Risikobewertung des Meldenden nachvollziehen und überprüfen kann.

- Angaben zur Einhaltung der Frist (wann hat sich der Vorfall ereignet, wann ist es dem Verantwortlichen zur Kenntnis gelangt).

- Alle Informationen zur Benachrichtigung nach Art. 34 DSGVO
  In der Meldepraxis fehlen sehr häufig Angaben dazu, ob der Betroffene benachrichtigt wurde und wenn nicht, warum nicht. Die Aussage, der Betroffene würde benachrichtigt, soweit es erforderlich ist, ist nicht zielführend.

- Alle Informationen zu den bereits getroffenen technisch-organisatorischen Maßnahmen zur Vermeidung weiterer solcher Datenpannen bzw. der beabsichtigten technisch-organisatorischen Maßnahmen mit Angabe der voraussichtlichen Umsetzung.

VI. Form der Meldung

Es ist keine besondere Form vorgeschrieben. In der Meldepraxis werden verschiedenste Formen gewählt. Entscheidend ist, dass die gewählte Form alle wesentlichen Inhalte enthält. Wir empfehlen die Nutzung des auf den BfDI-Webseiten zur Verfügungen gestellten Online-Formulars.

VII. Dokumentation nach Art. 33 Abs. 5 DSGVO

Der Verantwortliche hat die Verletzung des Schutzes personenbezogener Daten, die damit im Zusammenhang stehenden Fakten bzw. die für die Risikoprognose relevanten Umstände, die Auswirkungen der Verletzung und die ergriffenen Abhilfemaßnahmen zu dokumentieren. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen. Der BfDI ist berechtigt, sich diese Dokumentation vorlegen zu lassen. Von diesem Recht werden wir zukünftig vermehrt Gebrauch machen.

Die Dokumentationspflicht besteht unabhängig von der Meldepflicht.

VIII. Fazit

Die dargestellten Hinweise, insbesondere zum erforderlichen Inhalt einer Meldung nach Art. 33 DSGVO, bitte ich zu beachten. Darüber hinaus rate ich an, die in Ihrem Hause bestehende Meldepraxis nebst Formularen im Hinblick auf die genannten Aspekte zu überprüfen.

TOP 2: Mitarbeiterexzess

Mitarbeiterexzesse bzw. der Verdacht darauf gelangen dem BfDI in der Regel über eine Art. 33 DSGVO Meldung der Verantwortlichen zur Kenntnis. Das diesbezügliche Verfahren läuft „zweigleisig“: zum einen in Bezug auf den Mitarbeiterexzess an sich, zum anderen in Bezug auf die Frage, ob der meldende Verantwortliche im Umfeld des Mitarbeiterexzesses ange-

messene technisch-organisatorische Maßnahmen getroffen hatte. In beiden Verfahrensabschnitten haben wir Änderungen zum bisherigen Verfahren vorgenommen, worüber wir hiermit informieren möchten:

I. Was ist ein Mitarbeiterexzess?

Bei Mitarbeiterexzessen handelt es sich um Handlungen von Beschäftigten, die ausschließlich für dienst- oder betriebsfremde eigene Zwecke oder Zwecke eines Dritten erfolgen. Das ist dann der Fall, wenn die Handlung bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen bzw. dienstlichen Tätigkeit zugerechnet werden kann.

Daraus ergibt sich, dass im Hinblick auf den Verarbeitungsvorgang ein allgemein weisungswidriges Handeln des Mitarbeitenden für die Bejahung eines Mitarbeiterexzesses nicht ausreichend ist. Vielmehr muss eine Differenzierung vorgenommen werden, ob der Mitarbeitende den Verarbeitungsvorgang zu dienstlichen oder privaten Zwecken vorgenommen hat. Handelt ein Mitarbeitender zu privaten Zwecken weisungswidrig, verfolgt er eigene Zwecke und entscheidet über diese. Indem er sich hierfür des allenfalls für dienstliche Zwecke zur Verfügung gestellten Zugangs seines Dienstherrn bedient, entscheidet er zudem über die Mittel der Verarbeitung. Er schwingt sich dadurch für diesen Verarbeitungsvorgang selbst zum eigenständigen Verantwortlichen i.S.d. Art. 4 Nr. 7 DSGVO auf. In diesen Fällen liegt ein Mitarbeiterexzess vor, für dessen Verfolgung die jeweiligen Landesdatenschutzbeauftragten als Aufsichtsbehörden für den Privatsektor zuständig sind.

Die Behörde ist für den durch ihren Mitarbeitenden erfolgten Verarbeitungsvorgang datenschutzrechtlich nur insoweit verantwortlich, als dass sie verpflichtet ist, alle erforderlichen TOMs zu treffen, damit eine rechtswidrige Datenverarbeitung verhindert wird.

Handelt der Mitarbeitende hingegen zu dienstlichen Zwecken weisungswidrig, liegt kein Mitarbeiterexzess vor, d.h. die Behörde bleibt neben dem von ihr vorgenommenen Vorgang der Datenspeicherung auch für den Verarbeitungsvorgang ihres Mitarbeitenden datenschutzrechtlich verantwortlich und ihr wird der Verstoß weiterhin zugerechnet. Das betrifft insbesondere Fälle, in denen ein Mitarbeitender seine Befugnisse irrtümlich überschreitet.

II. Änderung der bisherigen Praxis

1. Feststellung eines Mitarbeiterexzesses

Zur Abgrenzung der Zuständigkeit des BfDI von der der Landesdatenschutzbeauftragten ist festzustellen, ob ein Mitarbeiterexzess vorliegt. Entscheidend ist hier ein privates Interesse des Mitarbeitenden an der Verarbeitung der Daten. Für die Bejahung eines Mitarbeiterexzesses und eine Anzeige an den Landesdatenschutzbeauftragten ist es ausreichend, dass genügend Anhaltspunkte für das Vorliegen eines privaten Interesses gegeben sind; eine „Ausermittlung“ des Sachverhalts durch BfDI wird nicht stattfinden.

Sofern sich aus der Meldung des Verantwortlichen jedoch nur das Überschreiten des zulässigen dienstlichen Rahmens des Verarbeitungsvorgangs ergibt, ist nicht eindeutig, ob sich die Handlung, etwa ein Datenbankzugriff, bei verständiger Würdigung der Umstände noch dem Kreis der dienstlichen Tätigkeit zuordnen lässt, oder sie zu privaten Zwecken des Beschäftigten erfolgte. Zukünftig wird in solchen Fällen eine Nachfrage bei der meldenden Stelle erfolgen und um Details zum Sachverhalt gebeten, die Aufschluss über die Motivation des Mitarbeiters geben können.

2. BfDI-Zuständigkeit gegenüber der meldenden Stelle

Im Hinblick auf ein mögliches Organisations- oder Überwachungsverschulden ist die Behörde Verantwortliche und der BfDI zuständig. Nach Art. 24 Abs. 1 DSGVO setzt der Verantwortliche geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt. Auch im Hinblick auf die Verhinderung möglicher Mitarbeiterexzesse hat die jeweilige Organisation als Verantwortliche die Einhaltung der DSGVO durch angemessene technische und organisatorische Maßnahmen sicherzustellen. Art. 32 Abs. 4 DSGVO verpflichtet den Verantwortlichen dazu, Schritte zu unternehmen, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf seine Anweisung verarbeiten. In Betracht kommen hier beispielsweise eine sorgfältige Auswahl zuverlässiger Mitarbeitender und die Schulung und Verpflichtung der Mitarbeitenden im Hinblick auf das Datengeheimnis,

sowie das Vorliegen von Berechtigungskonzepten und Konzepten zum Protokollieren des Zugriffs auf Datenbestände.

Die Einhaltung der technisch-organisatorischen Maßnahmen werden wir zukünftig regelmäßig beim Verantwortlichen nachfragen. Der Verantwortliche hat nach Art. 33 Abs. 5 S. 1 DSGVO neben der Verletzung des Schutzes personenbezogener Daten auch alle mit ihr zusammenhängenden Fakten sowie die Auswirkungen und deren Abhilfemaßnahmen zu dokumentieren. Dies erfordert auch die Dokumentation der Identität der den Exzess begehenden Person oder dessen Zugehörigkeit zu einer Abteilung. Wenn sich z.B. bei einem bestimmten Mitarbeitenden oder innerhalb einer bestimmten Abteilung Datenschutzvorfälle häufen, kann dies auf einen technisch-organisatorischen Mangel durch den Verantwortlichen hinweisen. Deshalb werden wir bei Verdacht auf einen Mitarbeiterexzess grundsätzlich die vom Verantwortlichen nach Art. 33 Abs. 5 DSGVO zu erstellende Dokumentation der Datenschutzverletzung anfordern.

III. Weiteres Verfahren in Bezug auf den Mitarbeiterexzess

Im Hinblick auf den sich zum Verantwortlichen aufschwingenden Mitarbeitenden besteht die Zuständigkeit der Landesdatenschutzbehörden, da diese für den Privatsektor zuständig sind. Bei allen Fällen, in welchen ein Mitarbeiterexzess vorliegt, entscheiden wir im Rahmen unseres pflichtgemäßen Ermessens, ob eine Anzeige an die zuständige Landesdatenschutzaufsicht erfolgt. Zuständig ist die Landesdatenschutzaufsicht, in dessen örtlichem Zuständigkeitsbereich der Mitarbeitende seinen Wohnsitz hat. Hierzu erfragen wir wie bisher vorab beim Verantwortlichen das Bundesland, in welchem der Mitarbeitende seinen Wohnsitz hat.

TOP 3: Zusammenarbeit mit dem BfDI

Unter diesem Tagesordnungspunkt wurde festgehalten, dass die Rundschreiben des BfDI weiterhin in regelmäßigen Abständen zu aktuellen datenschutzrechtlichen Themen verschickt werden. Geplant ist dabei ein halbjährlicher Rhythmus. Bei besonderem Anlass kann es zusätzliche Rundschreiben geben.

Im Übrigen soll die insgesamt gute Zusammenarbeit durch die ständige Etablierung des Formates des Runden Tisches sowie die regelmäßige Fortführung der verschiedenen jour fixes fortgeführt werden.

TOP 4: Anforderungen an die Verschlüsselung beim Austausch von Sozialdaten per E-Mail zwischen (Sozial-)Behörden

Die Frage, welche Anforderungen an die Verschlüsselung beim E-Mailversand von Sozialdaten zwischen Sozialbehörden zu stellen sind, wird kontrovers diskutiert. Seitens des BfDI wird auf die „Orientierungshilfe zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail" der DSK vom 27. Mai 2021 hingewiesen. Verantwortliche und Auftragsverarbeiter sind gesetzlich gehalten, die Risiken, die sich aus ihren Verarbeitungen personenbezogener Daten ergeben, hinreichend zu mindern. Sie müssen hierbei Art, Umfang, Umstände und Zwecke ihrer Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Mögliche Verschlüsselungswege sind die Transportverschlüsselung sowie die Ende-zu-Ende-Verschlüsselung. Sofern beide Behörden Teil des Regierungsnetzes sind, besteht eine qualifizierte Transportverschlüsselung, die für Daten mit normalem Risiko ausreichend ist. Bei Sozialdaten handelt es sich jedoch um besonders sensible Daten. Nach Auffassung des BfDI sollte beim Versand von Sozialdaten generell von einem hohen Risiko ausgegangen werden. Danach ist eine Transportverschlüsselung grundsätzlich nicht ausreichend; es sollte eine Ende-zu-Ende-Verschlüsselung erfolgen. Durch eine Ende-zu-Ende-Verschlüsselung mit den Verfahren S/MIME und OpenPGP ist es möglich, die Inhalte einer E-Mail-Nachricht durchgreifend gegen unbefugte Kenntnisnahme zu schützen. Dieser Schutz erstreckt sich dabei nicht nur auf den eigentlichen Transportweg, sondern auch auf die Zwischenspeicherung und -verarbeitung auf den an der Übermittlung beteiligten Servern.

TOP 5: IT-Verfahren der BA

Hinsichtlich der Rechtsfragen zur Verarbeitung und Übermittlung von Beschäftigtendaten (insbesondere kommunaler Beschäftigter der Jobcenter) verfolgen BA, BMAS und der BfDI das Ziel der Schaffung einer praktikablen und datenschutzfreundlichen Rechtsgrundlage. Es wird derzeit ein konkreter Entwurf für eine solche Übermittlungsbefugnis in § 44b SGB II abge-

stimmt. Auch eine Regelung zur Festlegung der datenschutzrechtlichen Verantwortlichkeiten bei Übertragung einer Aufgabe bzw. Inanspruchnahme einer Dienstleistung nach § 44b Abs. 4, 5 SGB II ist geplant. Hier besteht allerdings insbesondere für den Bereich der Personaldienstleistungen noch Klärungsbedarf. Grundsätzlich bestand zwischen allen Anwesenden (BMAS, BA, Vertreter der Jobcenter und BfDI) Konsens, dass eine Verteilung der Verantwortlichkeit im dem Sinn, dass die datenschutzrechtliche Ausgestaltung, Bereitstellung (und Durchführung) einer Dienstleistung/übertragenen Aufgabe in der Verantwortlichkeit der BA und die entsprechende datenschutzrechtliche Nutzung in der Verantwortlichkeit der jeweiligen Jobcenter liegt, zumindest die Sozialdaten betreffend, als sachgerecht empfunden wird. In diesem Sinne solle –vorbehaltlich einer Prüfung des jeweiligen Einzelfalls- eine Handhabung in der Praxis erfolgen, bis eine neue gesetzliche Regelung in Kraft getreten ist.

TOP 6: Umgang mit Verantwortlichen bei fehlender Einsicht von Datenschutzverstößen

TOP 6 setzte sich mit der Fragestellung auseinander, wie seitens der Datenschutzbeauftragten damit umgegangen werden kann, wenn sich die verantwortliche Stelle oder Beschäftigte dem Inhalt der Beratungen durch die behördlichen Datenschutzbeauftragten hinwegsetzen.

Die DSGVO regelt die Aufgaben und Befugnisse des Datenschutzbeauftragten. Nach Art. 39 Abs. 1a) DSGVO obliegt dem Datenschutzbeauftragten die Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten. Mit der Beratung ist demnach der gesetzlichen Pflicht genüge getan. Die erfolgte Beratung sollte zu Dokumentationszwecken schriftlich festgehalten werden.

Die Datenschutzbeauftragten haben zudem ein Vorsprachrecht bei der Geschäftsführung. Dieses sollte ebenfalls protokolliert werden und in den Tätigkeitsbericht aufgenommen werden. Daraufhin kann auch die Trägerversammlung tätig werden.

Darüber hinaus besteht auch jederzeit die Möglichkeit, sich an den BfDI als zuständige Aufsichtsbehörde zu wenden.

TOP 7: Zugriffe auf Allegro und Falke

Unter diesem Tagesordnungspunkt wurden die Zugriffsberechtigungen auf die Fachverfahren Allegro und Falke besprochen.

Den Jobcentern sei aufgefallen, dass die Leistungssachbearbeiter Allegro-Fälle bundesweit öffnen könnten, während die E-Leistungsakte nur im jeweils zuständigen Jobcenter geöffnet werden kann.

Im Fachverfahren Falke seien über die Suchfunktion alle Verfahren der einzelnen Kunden einsehbar.

Die BA hat zugesagt, die Zugriffsberechtigungen für beide Fachverfahren zu prüfen. Die Zugriffsberechtigungen können aber auch wegen falscher Rollenkonzepte der betreffenden Jobcenter gegeben sein. Darüber hinaus sei in bestimmten fachlichen Konstellationen ein übergreifender Zugang erforderlich.

Die BA hat zugesagt, beide Fachverfahren auf die erforderlichen Zugriffsberechtigungen hin zu überprüfen und wird dieses Ergebnis dann sowohl dem BMAS als auch dem BfDI mitteilen.

TOP 8: Position des behördlichen Datenschutzbeauftragten, Unterstellung unter eine Führungskraft

Für viele Datenschutzbeauftragte ist die Frage entscheidend, ob sie in Ihrer Funktion in ein Team eingegliedert werden können oder als Stabsstelle direkt der Geschäftsführung unterstellt sind.

Die unabhängige und organisatorisch herausgehobene Stellung ist für eine wirkungsvolle Tätigkeit des Datenschutzbeauftragten von ausschlaggebender Bedeutung. Er darf bei der Wahrnehmung seiner Aufgaben keinen Weisungen unterliegen – weder solchen von Vorgesetzten noch solchen der Organisationseinheiten, die er zu kontrollieren hat. Außerdem verlangt Art. 38 Abs. 3 DSGVO ein direktes Vorspracherecht bei der Geschäftsführung. Die DSGVO enthält keine konkreten Vorgaben hinsichtlich der organisatorischen Stellung des Datenschutzbeauftragten. Demnach ist grundsätzlich zwar eine Eingliederung der Datenschutzbeauftragten „in der Linie“ möglich, sofern die Weisungsfreiheit und das Berichtsrecht nicht be-

einträchtigt werden. Der BfDI empfiehlt jedoch eine Einrichtung als Stabsstelle, die der Geschäftsführung direkt unterstellt ist.

Um die Unabhängigkeit der Datenschutzbeauftragten nicht zu gefährden, empfiehlt der BfDI, dass diese, wenn sie zu 100% freigestellt sind, auch nicht dienstrechtlich beurteilt werden, sondern –wie bei Mitgliedern der Personalvertretung- eine fiktive Laufbahnnachzeichnung vorzunehmen ist. Etwas anderes ergibt sich bei einer nur teilweisen Freistellung für die Beurteilung der nicht dem Amt des behördlichen Datenschutzbeauftragten zuzuordnenden Tätigkeit.

Es besteht weiterhin ein großes Bedürfnis nach klaren Vorgaben zur tarifrechtlichen Eingruppierung der Datenschutzbeauftragten. Da es sich letztlich um ein tarif- bzw. besoldungsrechtliches Thema handelt, steht der BfDI grundsätzlichen Vorgaben zurückhaltend gegenüber. Bei Konflikten können sich die Datenschutzbeauftragten jedoch an den BfDI wenden, worauf dann der konkrete Einzelfall geprüft werden kann.

TOP 9: Sonstiges

a) Übersetzungsgeräte in den Jobcentern

Dem BfDI ist durch Datenpannenmeldungen nach Art. 33 DSGVO zur Kenntnis gelangt, dass verschiedene Jobcenter elektronische Geräte nutzen oder genutzt haben, die gesprochene Sprache simultan übersetzen können. Dabei fließen Daten über verschiedene, gegebenenfalls auch ausländische Server, ohne dass eine Übermittlungsbefugnis gegeben ist.

Der BfDI empfiehlt dringend, den Einsatz dieser Übersetzungsgeräte umgehend einzustellen bzw. nur solche Geräte zu nutzen, die datenschutzkonform betrieben werden können.

b) Löschen von E-Mails

Die Löschfrist von E-Mails in den Teampostfächern bemisst sich grundsätzlich nach der allgemeinen Löschfrist für Sozialdaten. Hier sind keine konkreten Vorgaben durch die BA möglich. Der BfDI empfiehlt die Erstellung eines Löschkonzepts.

c) Google Rezensionen

Soweit Behörden mit einem (Unternehmens-)Profil bei Google hinterlegt sind, besteht die Möglichkeit für Dritte, Bewertungen vorzunehmen. Hierbei kann es zu negativen Bewertungen kommen, die mitunter unangemessene, manchmal auch strafrechtlich relevante Inhalte haben. Das ist in erster Linie kein datenschutzrechtliches Problem. Soweit es durch eine Bewertung zu Rechtsverstößen kommt, kann von Google die Löschung verlangt werden. Erfolgsversprechend ist ein Löschbegehren insbesondere, wenn ein Verstoß der Bewertung gegen die Compliance-Richtlinien von Google vorliegt.

II. Klarstellung zum Bericht zum Runden Tisch 2022 (Rundschreiben 09/2022)

Im o.g. Rundschreiben haben wir zu TOP 5 (Unverschlüsselte E-Mail-Kommunikation) auf den DSK-Beschluss vom 24.11.2021 „zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen“ hingewiesen. Wir haben ausgeführt, dass laut DSK-Beschluss im Einzelfall ausnahmsweise vom Grundsatz, dass Einwilligungen in den Verzicht auf technisch organisatorische Maßnahmen nicht möglich sind, abgewichen werden kann, wenn u.a. folgende Voraussetzung erfüllt ist: „Eine unverschlüsselte E-Mail-Kommunikation kann nur im Einzelfall erfolgen. Eine solche darf keinesfalls regelmäßig erfolgen.“

Klarstellend ist hier anzumerken, dass nach Ansicht des BfDI auch die Fälle als Einzelfall im Sinne des DSK-Beschlusses gewertet werden können, in denen es um wiederkehrende Schriftwechsel mit der identischen betroffenen Person zu im wesentlichen identischen Lebenssachverhalten geht und für die die übrigen Voraussetzungen des DSK-Beschlusses (u.a.: Wunsch nach unverschlüsselter Kommunikation muss vom Kunden selbst ausgehen) geprüft und bejaht wurden.

Abschließend möchte ich die Gelegenheit nutzen und Ihnen ein frohes Weihnachtsfest und einen guten Rutsch ins neue Jahr wünschen! Der 3.

Runde Tisch zum Datenschutz in der Arbeitsverwaltung wird voraussichtlich im September oder Oktober 2024 stattfinden.

Mit freundlichen Grüßen
Im Auftrag

Dr. Olaf Kisker