Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

[redacted]
Abteilungsleiterin 3

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

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON [redacted]
E-MAIL [redacted]
BEARBEITET VON [redacted]
INTERNET www.bfdi.bund.de

DATUM Bonn, 09.05.2023
GESCHÄFTSZ. 36-623-4/003#0033

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

[redacted]

nachrichtlich:

[redacted]

Bundesministerium für Wirtschaft
und Klimaschutz
Referat ZC 3
ausschließlich per E-Mail:
[redacted]

Bundesministerium für Wirtschaft
und Klimaschutz
Referat ZC 2
ausschließlich per E-Mail:
[redacted]

BETREFF **Beratungs- und Kontrollbesuch bei [redacted] im Zeitraum 28. bis 30. März 2023 zur Überprüfung der datenschutzrechtlichen Vorgaben des Sicherheitsüberprüfungsgesetzes (SÜG)**

HIER Ergebnis meiner Kontrolle

Sehr geehrter [redacted],

vom 28. bis 30. März 2023 führte ich bei [redacted] einen Kontroll- und Beratungsbesuch gemäß § 36a Abs. 2 und 3 des Gesetzes

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

über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG) i. V. m. § 36 Abs. 1 SÜG, § 16 Abs. 2 Bundesdatenschutzgesetz (BDSG) zum Umgang mit personenbezogenen Daten im Rahmen von Sicherheitsüberprüfungen durch.

Gegenstände meiner Kontrolle waren:

- personelle Ausstattung und Verfahrensabläufe im Bereich Geheimschutz,
- örtliche Gegebenheiten (Zutrittsrechte, Aufbewahrung und Vernichtung der Akten),
- Informationsflüsse zwischen den Bereichen Geheimschutz und personalverantwortlicher Stelle,
- Inhalt der Sicherheitsakten (Stichprobe von 117 Akten),
- Elektronische Datenverarbeitung zu den Sicherheitsüberprüfungsverfahren.

Weitere Sachverhalte außerhalb des oben genannten Kontrollgegenstandes wurden nicht geprüft.

Seitens [redacted] waren der Konzern-Sicherheitsbevollmächtigte, zugleich Konzern-Sabotageschutzbevollmächtigter (im Folgenden: SiBe) und seine beiden Stellvertretenden maßgeblich an der Kontrolle beteiligt.

Für die meinen Mitarbeitenden gewährte Unterstützung im Vorfeld und während der Kontrolle, die offene, kooperative und sehr freundliche Gesprächsatmosphäre, die Bereitschaft, Anregungen aufzunehmen und notwendige Änderungen umzusetzen, danke ich insbesondere den oben genannten Mitarbeitern von [redacted].

I. Ergebnis meiner Kontrolle

Die Kontrolle ergab, dass nicht alle Verarbeitungen mit den datenschutzrechtlichen Anforderungen im Einklang stehen. Die Mängel betreffen die interne Kommunikation nach § 15 a SÜG, Inhalte der Sicherheitsakten und der elektronischen Datei sowie die Verfahrensdokumentation hinsichtlich der Vernichtung und Löschung von Sicherheitsakten.

Sofern nicht zugesagt wird, in angemessener Frist entsprechende Abhilfemaßnahmen zu treffen, behalte ich mir den Erlass von Beanstandungen vor:

1. Zur Sicherstellung der Aufgabenerfüllung nach dem SÜG hat die personalverwaltende Stelle zukünftig ihren aus §§ 29 Abs. 2 Satz 1, 15a SÜG auferlegten Pflichten vollumfänglich nachzukommen.

2. In der Sicherheitserklärung sind zukünftig ausschließlich die nach § 13 SÜG für die vorgesehene Art der Sicherheitsüberprüfung erforderlichen personenbezogenen Daten zu erheben. Die bereits ohne Rechtsgrundlage erhobenen Daten sind dauerhaft unkenntlich zu machen.

3. Die Sicherheitserklärung ist gem. § 30 i. V. m. § 18 Abs. 1 SÜG vollständig in der Sicherheitsakte aufzubewahren. Die gemäß § 2 Abs. 1 Satz 2 und 3 SÜG i. V. m. § 36 Abs. 1 Nr. 2 SÜG, § 51 Abs. 1 BDSG für die Durchführung der Sicherheitsüberprüfung erforderliche Zustimmung kann ansonsten nicht nachgewiesen werden. Die Sicherheitsakte ist insoweit zu ergänzen.

4. Die Verarbeitung und Speicherung personenbezogener Daten in einer elektronischen Datei i. S. d. § 31 SÜG hat sich auf das zulässige Maß zu beschränken, nämlich, wenn diese zur Erfüllung der Aufgaben nach dem SÜG erforderlich sind. Hierzu zählt der akademische Titel in der Regel nicht. Sofern keine Einwilligung zur Datenverarbeitung der betroffenen Person in die elektronische Datenverarbeitung eingeholt werden kann, sind die Eintragungen mangels Rechtsgrundlage zu löschen.

5. In den aufbewahrungspflichtigen Sicherheitsakten ist stets das Datum des Ausscheidens aus der sicherheitsempfindlichen Tätigkeit korrekt zu dokumentieren und das hieraus folgende Vernichtungsdatum gemäß §§ 30, 19 Abs. 2 und 31 Satz 2, 22 Abs. 2 Nr. 1 SÜG zu berechnen und in der Sicherheitsakte tagesgenau zu dokumentieren (§ 30 i. V. m. § 18 SÜG).

Darüber hinaus spreche ich folgende Empfehlung aus:

6. Soweit der Hinweis auf eine bestehende Gehörlosigkeit als Bearbeitungshinweis zur Aufgabenerfüllung erforderlich ist, sollte in einer elektronischen Datei i. S. d. § 31 SÜG ein neutraler Vermerk ohne Aufnahme des Gesundheitsdatums (z.B. „keine telefonische Kontaktaufnahme möglich“) gespeichert werden.

II. Sachverhalt

Die nachfolgenden Feststellungen beruhen auf den Antworten des SiBe von [redacted] auf meinen Fragebogen, den Erkenntnissen meiner Mitarbeitenden aus den Gesprächen vor Ort, einer Aktenstichprobe sowie der Sichtung von Datensätzen in der von [redacted] genutzten Datenbank, in der auch VS-NfD-belehrtes Personal geführt wird.

Nach Mitteilung von [redacted] führte das Unternehmen am Stichtag 27. Februar 2023 insgesamt 3.104 Sicherheitsakten am Standort [redacted], darunter 104 Akten zu Antragsverfahren

und 837 Akten von ausgeschiedenen Personen. Meine Kontrolle umfasste 117 Aktenvorgänge zzgl. einer Stichprobe der Dateien, darunter

- 67 ermächtige Beschäftigte,
- 47 aus der sicherheitsempfindlichen Tätigkeit ausgeschiedene Personen,
- 3 Antragsverfahren.

Sofern Widersprüche gegen die Einsichtnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) gemäß § 36a Abs. 2 SÜG vorlagen, waren die betreffenden Sicherheitsakten bereits durch den SiBe gekennzeichnet und von einer Einsichtnahme durch den BfDI ausgenommen.

Soweit im Folgenden auf einzelne Sicherheitsakten eingegangen wird, sind diese mittels der von mir während der Kontrolle geführten Fallliste (FL) mit der jeweiligen Ordnungsnummer identifizierbar. Die Fallliste wird mit separatem Schreiben ausschließlich an den SiBe von [redacted] sowie an die Fachreferate ZC2 und ZC3 des BMWK übersandt.

1. Interne Kommunikation nach § 29 i. V. m. § 15 a SÜG

Der SiBe erhält seitens der personalverwaltenden Stelle (HR) einzig Mitteilung über Änderungen folgender personenbezogene Daten (sog. Stammdaten aus SAP): Anrede, Vorname, Nachname, Nationalität, Anschrift, interne Telefonnummer und das Ausscheiden der Mitarbeitenden aus dem Unternehmen. Dies erfolgt durch monatliches Überspielen der Datensätze in die Fachanwendung SeCon durch den SiBe. Hierfür hat [redacted] folgenden Prozess konzipiert: Die personalverwaltende Stelle übermittelt die Stammdaten aus SAP einmal monatlich an [redacted]. Mittels USB-Stick holt der SiBe die Datensätze ab und überspielt sie auf SeCon. So wird sichergestellt, dass regelmäßig die Stammdaten in SeCon aktualisiert werden.

Zu seiner Absicherung erfragt der SiBe bei jedem Ausscheiden bei HR noch einmal explizit ab, ob die betroffene Person tatsächlich ausgeschieden ist und zu welchem Zeitpunkt.

In einem Fall war die Namensänderung zwar überschrieben worden, ist dem SiBe aber aktiv nicht aufgefallen (FL. 57). Die Veränderungsmitteilung an das BMWK wurde noch während der Kontrolle abgesetzt.

Eine Mitteilung über interne Versetzungen erfolgt nicht, was zum Zeitpunkt des Kontrollbesuchs bereits seitens [redacted] erkannt war und derzeit überarbeitet wird.

Weitere Informationen, insbesondere über sicherheitserhebliche Erkenntnisse gemäß § 29 Abs. 2 i. V. m. § 15 a SÜG, werden dem SiBe seitens HR nicht mitgeteilt.

Neben dem sicherheitsüberprüften Personal werden auch die personenbezogenen Daten aller VS-NfD-belehrten Mitarbeitenden elektronisch in SeCon verarbeitet, wobei der Belehrungsnachweis in der Personalakte gespeichert ist. In einem dieser Fälle war SAP durch HR falsch gepflegt worden, weshalb der „Austritt“ durch Versterben des Mitarbeitenden nicht übermittelt wurde (FL 118). In SeCon wurde der Datensatz bereits vor Ort durch den SiBe gelöscht. Der Belehrungsnachweis befindet sich nach wie vor in der Personalakte und wurde bislang nicht vernichtet.

In einem Fall hatte sich im Jahre 2015 bei einem Betroffenen eine Adressänderung ergeben. Aber erst im Rahmen der Aktualisierungsüberprüfung 2018 ist aufgefallen, dass sich die Anschrift der betroffenen Person zwischenzeitlich geändert hatte.[1]

2. Personenbezogene Daten unbeteiligter Dritter in der Sicherheitserklärung

In zwei Akten enthielten die jeweiligen Sicherheitserklärungen personenbezogene Daten zu minderjährigen Kindern (FL 13, 22).

3. Fehlende Dokumentation der Zustimmung zur Durchführung der Sicherheitsüberprüfung

Die in der Sicherheitsakte mit der FL-Nr. 50 enthaltene erste Sicherheitserklärung aus dem Jahre 2005 war nur unvollständig veraktet, insbesondere fehlte die letzte Seite der Sicherheitserklärung, auf der die betroffene Person ihre Einwilligung in die Durchführung der Sicherheitsüberprüfung erteilt hatte sowie das zugehörige Datum.

Meine Rückfrage beim BMWK ZC2 ergab, dass dort die entsprechende Sicherheitserklärung einschließlich Unterschriften vollständig in der Sicherheitsakte abgelegt ist.

4. Umfang der elektronischen Verarbeitung personenbezogener Daten

Die kontrollierte Stelle verwendet zur Vorgangsverwaltung die Fachanwendung SeCon auf einem Standalone-System. Darin ist unter anderem das Feld „Titel“ vorgesehen, wobei der

[1] Der Fall wurde nicht in die Prüfliste aufgenommen, da hier kein Nachbesserungsbedarf mehr besteht.

akademische Titel gemeint ist. Der SiBe befüllte das Feld regelmäßig auch in den Fällen, in denen die betroffene Person nicht am Besuchskontrollverfahren teilnimmt.

In einem Fall fand sich in SeCon unter „Kurzbemerkung“ die Eintragung „gehörlos“ (FL 31). Die Eintragung wird laut SiBe in allen Fällen der Gehörlosigkeit in SeCon vorgenommen. Hintergrund sei, dass in diesen Fällen eine Kontaktaufnahme zur betroffenen Person nur schriftlich erfolgen könne und nicht – wie üblich – telefonisch.

5. Berechnung der Vernichtungsfrist und Dokumentation des Vernichtungsdatums

In 8 Fällen (FL 90-96, 100) war das fristauslösende Ereignis zur Bestimmung der Vernichtungsfrist nicht korrekt bestimmt und in der Folge nicht korrekt an das BMWK übermittelt worden:

In den Fällen 90-95 war die betroffene Person zum 01.10.2018 aus der sicherheitsempfindlichen Tätigkeit ausgeschieden. Mit Veränderungsmitteilung an das BMWK wurde der 02.10.2018 als Datum des Ausscheidens mitgeteilt. In den Fällen FL 91-95 war in SeCon ebenfalls der 02.10.2018 als Datum des Ausscheidens vermerkt. Im Fall FL 90 war in SeCon kein Datum des Ausscheidens vermerkt.

Im Fall 96 war die betroffene Person zum 31.08.2018 aus der sicherheitsempfindlichen Tätigkeit ausgeschieden. Mit Veränderungsmitteilung an das BMWK wurde der 23.10.2018 als Datum des Ausscheidens mitgeteilt (die betroffene Person hatte die Entmächtigung am 22.10.2018 unterzeichnet). In SeCon war als Austrittdatum der 23.10.2018 vermerkt.

Im Fall 100 war die betroffene Person zum 13.11.2018 ausgeschieden. Mit Veränderungsmitteilung an das BMWK wurde der 26.11.2018 als Datum des Ausscheidens mitgeteilt. In SeCon wurde der 26.11.2018 als Datum des Ausscheidens vermerkt.

In keiner der kontrollierten Sicherheitsakten war das (taggenaue) Vernichtungsdatum auf oder in der Sicherheitsakte dokumentiert (FL 72-117).

Die mit einer fünfjährigen Vernichtungsfrist zur Vernichtung anstehenden Sicherheitsakten (FL 78-117) waren vielmehr nach dem Monat und Jahr des Ausscheidens in einem Aktenschrank gesondert abgelegt und sortiert. Die mit einer Jahresfrist zur Vernichtung anstehenden Sicherheitsakten (FL 72-77) waren hiervon getrennt nach demselben Prinzip abgelegt.

Die Akten wurden inzwischen vernichtet.

III. Rechtliche Bewertung

Gemäß §§ 36a Abs. 2 und 3, 36 SÜG ist der BfDI für die Datenschutzaufsicht bei den öffentlichen und nichtöffentlichen Stellen, die Aufgaben nach dem SÜG erfüllen, zuständig.

Nach § 36 Abs. 1 SÜG i. V. m. § 16 Abs. 2 Satz 1 BDSG bin ich befugt, Verstöße gegen das BDSG oder gegen andere Datenschutzvorschriften oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten gegenüber der zuständigen obersten Bundesbehörde zu beanstanden.

Die Voraussetzungen sind vorliegend erfüllt.

Zu den Feststellungen im Einzelnen:

1. Interne Kommunikation nach §§ 29 Abs. 2 Satz 1, 15 a Satz 1 SÜG

Gemäß §§ 29 Abs. 2 Satz 1, 15a Satz 1 SÜG hat die personalverwaltende Stelle den für die Sicherheitsüberprüfung zuständigen SiBe unverzüglich über Veränderungen der persönlichen, dienstlichen und arbeitsrechtlichen Verhältnisse der Personen zu unterrichten, wenn diese mit einer sicherheitsempfindlichen Tätigkeit betraut werden sollen oder bereits betraut sind.

Die personalverwaltende Stelle ist somit gesetzlich verpflichtet, den SiBe zu unterstützen. Die Pflicht trifft die personalverwaltende Stelle unverzüglich, vom Zeitpunkt der Einleitung einer Sicherheitsüberprüfung bis die betroffene Person aus der sicherheitsempfindlichen Tätigkeit ausscheidet.

Nach meinen Feststellungen besteht kein ausreichender Informationsfluss durch die personalverwaltende Stelle der [redacted] an den SiBe.

Der SiBe erfährt lediglich von Veränderungen der Anrede, des Vor- und Nachnamens, der Anschrift, Nationalität, internen Erreichbarkeit und über das Ausscheiden aus dem Unternehmen. Informationen zu Vorstrafen, arbeitsrechtlich relevanten Vorkommnissen, Personenstandsänderungen, Überschuldung (nur erforderlich im personellen Geheimschutz) etc. erhält der SiBe nicht. Auch wenn die betroffene Person intern versetzt wird und dabei beispielsweise aus der sicherheitsempfindlichen Tätigkeit ausscheidet, wird der SiBe hierüber nicht durch HR in Kenntnis gesetzt. Die personalverwaltende Stelle kommt folglich ihrer gesetzlichen Informationspflicht aus §§ 29 Abs. 2 Satz 1, 15a Satz 1 SÜG nicht vollumfänglich nach.

Das derzeitige Informationsmanagement durch den monatlichen Abgleich von SAP und SeCon, erfüllt zudem nicht die Anforderungen aus § 36 Abs. 1 Nr. 2 SÜG i.V.m. § 64 BDSG. Nach § 36 Abs. 1 Nr. 2 SÜG i.V.m. § 64 BDSG hat die verantwortliche Stelle unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten.

Die interne Sicherstellung erforderlicher Datenübermittlungen innerhalb des Unternehmens ist in erster Linie ein Baustein organisatorischer Maßnahmen. Hierbei kann sich die verantwortliche Stelle technischer Hilfsmittel bedienen, wie etwa vorliegend durch den monatlichen Datentransfer von SAP zu SeCon geschehen. Meine Feststellungen lassen jedoch den Schluss zu, dass der monatliche Datentransfer **allein** nicht geeignet ist, das gesetzlich geforderte angemessene Schutzniveau zu gewährleisten. Dies selbst dann nicht, wenn zukünftig zusätzliche Datenfelder unter den monatlichen Abgleich gefasst würden.

Dies liegt zum einen daran, dass beide Dateisysteme unterschiedliche Daten als fristauslösendes Ereignis bewerten: So erfasst HR in SAP im Falle des Ausscheidens den endgültigen Austritt aus dem Unternehmen (Ende des Arbeitsverhältnisses, Eintritt Ruhestand). Im Bereich des personellen Geheim- und Sabotageschutzes hingegen ist für die Berechnung des Vernichtungsdatums der Zeitpunkt relevant, in dem die betroffene Person die sicherheitsempfindliche Tätigkeit tatsächlich nicht mehr ausübt. Dies kann ein abweichendes Datum sein. So stellt etwa bei Erkrankung, Resturlaubsansprüchen vor Ende des Arbeitsverhältnisses bzw. Eintritt in den Ruhestand, Elternzeit etc. der letzte Arbeitstag in der sicherheitsempfindlichen Tätigkeit das fristauslösende Ereignis für die Vernichtung bzw. Löschung dar. Somit ist der SiBe gezwungen, aktiv bei HR das für ihn relevante Datum abzufragen. Soweit der SiBe generell bei jedem Austritt von sich aus gesondert bei HR Nachforschungen zum für ihn relevanten Datum des Ausscheidens anstellt, kompensiert er hier eigeninitiativ den fehlenden Informationsfluss. Dies ersetzt jedoch nicht die Informationspflicht aus § 15 a SÜG und ist überdies bei einem derart hohen SÜ-Fallaufkommen wie bei [redacted] und dem Umstand, dass der SiBe abgesehen von seinen beiden Stellvertretern keine weitere personelle Unterstützung an seiner Seite hat, nicht risikoangemessen (siehe hierzu weitere Ausführungen unten).

Andererseits ist bei der Datenübermittlung die Grundvoraussetzung, dass SAP durch HR auch korrekt gepflegt ist. Die unter Ziffer II.1. genannten Fälle belegen, dass das System

fehleranfällig ist und es hier zur Datenschutzverstößen kommen kann. So ist die VS-NfD-Belehrung genauso wie die Sicherheitsakte bei Versterben der betroffenen Person sofort zu vernichten (FL 118). Gemäß § 19 Abs. 2 SÜG analog hat der SiBe auch die fristgerechte Löschung des Datensatzes VS-NfD-belehrter Mitarbeitenden zu verantworten und ist hierbei auf Informationen über das Ausscheiden seitens HR angewiesen (FL 118).

Ebenfalls muss der SiBe relevante Änderungen aktiv zur Kenntnis nehmen können, um beispielsweise seine Handlungspflichten gegenüber der zuständigen Stelle, dem BMWK, auch erfüllen zu können. Der monatliche Datenabgleich zwischen SAP und SeCon berücksichtigt den gesamten Mitarbeiterbestand von mehreren Tausend Datensätzen. Die Datensätze des SiBe umfassen zum einen die Mitarbeitenden die eine sicherheitsempfindliche Tätigkeit nach dem SÜG ausüben und jene, die mittels VS-NfD-Verpflichtung belehrt sind (dies betrifft alle übrigen Beschäftigten). Im Rahmen der vergleichsweise geringen Personalausstattung kann dem SiBe nicht zugemutet werden, dass er bei Stammdatenänderungen, die alle Mitarbeitenden betreffen und die in der Regel systemseitig angezeigt werden, für sich filtert, welche Informationen nach § 15 a SÜG relevant sind. Die kontrollierten und geschilderten Sachverhalte der Namens- und Adressänderung belegen, dass systemseitig angezeigte Stammdatenänderungen/Informationen in der Masse untergehen können. Dem SiBe ist die Anschriftenänderung der betroffenen Person erst im Rahmen der Aktualisierungsüberprüfung aufgefallen und er konnte seiner Mitteilungspflicht gegenüber dem BMWK daher nur nachträglich nachkommen. Die Namensänderung fiel zufällig im Rahmen dieser Kontrolle auf. Durch den alleinigen Datenabgleich können also wichtige Informationen verloren gehen, die im Einzelfall auch sicherheitsrelevant sein können.

Die datenschutzrechtliche Relevanz des fehlenden Informationsflusses ergibt sich, wenn sich tatsächliche Umstände ändern und personenbezogene Daten in der Sicherheitsakte (des SiBe und folglich auch des BMWK) unrichtig werden oder sobald die zu übermittelnden Informationen fristauslösende Ereignisse betreffen und damit für die zulässige Speicherdauer relevant sind.

So kann der SiBe, wenn er nicht erfährt, wann eine Person aus der sicherheitsempfindlichen Tätigkeit ausgeschieden ist, die Vernichtungsfrist nicht nach den datenschutzrechtlichen Vorgaben des SÜG berechnen. Dadurch drohen Verstöße gegen Vernichtungsfristen.

Die personalverwaltende Stelle hat daher zukünftig ihren aus §§ 29 Abs. 2 Satz 1, 15a SÜG auferlegten Pflichten vollumfänglich nachzukommen.

Insofern sich der VS-NfD-Belehrungsnachweis der verstorbenen Person nach wie vor in der Personalakte befindet, bitte ich um Löschung des Dokumentes (FL 118).

2. Personenbezogene Daten unbeteiligter Dritter in der Sicherheitserklärung

Die Verarbeitung personenbezogener Daten bedarf stets einer Rechtsgrundlage. Welche Angaben in der Sicherheitserklärung von der betroffenen Person zu machen sind, regelt § 13 SÜG abschließend.

Gem. § 13 Abs. 1 Nr. 9 SÜG sind in der Sicherheitserklärung nur im Haushalt lebende Personen anzugeben, die über 18 Jahre alt sind. Im Haushalt lebende minderjährige Kinder sind nicht anzugeben.

Nach § 26 Satz 4 SÜG ist der SiBe verpflichtet, die Sicherheitserklärung auf Vollständigkeit und Richtigkeit zu prüfen. Dazu gehört auch, dass die Sicherheitserklärung nicht mehr Daten enthält als zulässig erhoben werden dürfen.

Die in den Sicherheitserklärungen ohne Rechtsgrundlage erhobenen Daten sind daher nachträglich unkenntlich zu machen (FL 13, 22). Zukünftig ist darauf zu achten, dass die betroffene Person nur erforderliche Daten in der Sicherheitserklärung angibt.

3. Fehlende Dokumentation der Zustimmung zur Durchführung der Sicherheitsüberprüfung

Gemäß §§ 30, 18 Abs. 1 SÜG sind in die Sicherheitsakte der betroffenen Person alle die Sicherheitsüberprüfung betreffenden Informationen aufzunehmen. So nimmt die oder der SiBe eine Kopie der Sicherheitserklärung zur Sicherheitsakte (Nr. 4.2.3 Abs. 4 und Nr. 4.7.2 Abs. 1 des Geheimschutzhandbuchs des BMWK). Insbesondere bildet die unterschriebene Sicherheitserklärung die Rechtsgrundlage für die Durchführung des Überprüfungsverfahrens mit all seinen erforderlichen Maßnahmen. Darüber hinaus muss die datenverarbeitende verantwortliche Stelle gemäß § 36 Abs. 1 Nr. 2 SÜG i. V. m. § 51 Abs. 1. BDSG die gemäß § 2 Abs. 1 Satz 2 und 3 SÜG erforderliche Einwilligung zur Datenverarbeitung nachweisen können. Auch dies ist nicht möglich, wenn die ursprüngliche Sicherheitserklärung nur unvollständig veraktet ist und die darin per Unterschrift erteilte Zustimmung fehlt.

In der Sicherheitsakte mit der FL-Nr. 50 war die erste Sicherheitserklärung aus dem Jahre 2005 nicht vollständig veraktet, insbesondere fehlte die letzte Seite mit dem Datum und der Unterschrift der (mit-)betroffenen Person. Das BMWK teilte mir mit, die Sicherheitserklärung läge in der dortigen korrespondierenden Sicherheitsakte vor. Das BMWK hat zugesagt, eine vollständige Kopie an [redacted] zu übersenden, sodass mit Hilfe dieser die Sicherheitsakte durch [redacted] vervollständigt werden kann. Ich bitte um Bestätigung der Umsetzung.

Zukünftig ist sicherzustellen, dass die Sicherheitsakte vollständig geführt wird.

4. Umfang der elektronischen Verarbeitung personenbezogener Daten

§ 31 Satz 1 SÜG regelt abschließend, welche Daten die nichtöffentliche Stelle im Rahmen der Aufgabenwahrnehmung in Dateien speichern darf. Demnach dürfen nur solche personenbezogenen Daten in einer automatisierten Datei gespeichert werden, die zur Erfüllung der Aufgaben nach dem SÜG erforderlich sind. Zur Erfüllung der Aufgaben nach dem SÜG erforderlich sind insbesondere die Daten, die gemäß den §§ 26 bis 29 SÜG verarbeitet werden dürfen. §§ 26, 13 SÜG i. V. m. § 11 f. SÜG regelt abschließend, welche Informationen mit der Sicherheitserklärung erhoben werden dürfen. Personenbezogene Daten, die mangels Rechtsgrundlage nicht erhoben werden dürfen, sind für die Erfüllung der Aufgaben nach dem SÜG nicht erforderlich. Dementsprechend darf das Datenfeld „Titel“ nicht mit dem akademischen Grad der betroffenen Personen befüllt werden.

Der akademische Grad in Form des Dr.-Titels fällt nicht unter § 13 Abs. 1 SÜG. Insbesondere handelt es sich hierbei weder um einen Bestandteil des Namens (§ 13 Abs. 1 Satz 1 Nr. 1 SÜG) noch um eine Berufsbezeichnung (§ 13 Abs. 1 Satz 1 Nr. 6 SÜG). Bei dem Dr.-Titel handelt es sich um eine Abschlussbezeichnung gemäß Stufe 8 des Europäischen Qualifikationsrahmens für lebenslanges Lernen der EU, die von dazu berechtigten Hochschulen aufgrund eines erfolgreich mit einer Hochschulprüfung abgeschlossenen Studiums oder aufgrund einer besonderen wissenschaftlichen Leistung vergeben und durch eine Urkunde dokumentiert werden (Graduierung); vgl. hierzu § 4 Abs. 1 Nr. 3 Passgesetz und § 5 Abs. 2 Nr. 3 Personalausweisgesetz.

Bei betroffenen Personen, die am Besuchskontrollverfahren teilnehmen, war die Einwilligung in die Verarbeitung des Dr.-Titels durch die Zusatzvereinbarung zum Arbeitsvertrag im personellen Geheimschutz dokumentiert. Bei den übrigen sicherheitsüberprüften Mitarbeitenden lagen hingegen keine Anhaltspunkte dafür vor, dass es sich um eine zusätzliche, freiwillige Angabe handelt, die auf der Grundlage einer Einwilligung erhoben und verarbeitet wurde.

Dementsprechend sind die vorhandenen Einträge entweder zu löschen und künftig nicht mehr zu speichern oder es ist in den einschlägigen Fällen eine entsprechende Einwilligung nachträglich einzuholen und zukünftig sicherzustellen, dass eine ordnungsgemäße Einwilligung dokumentiert wird. Hierbei ist zu beachten, dass dies auch für den Bereich des vorbeugenden personellen Sabotageschutzes gilt.

Den bereits erstellten Formulierungsvorschlag des SiBe zur Ausgestaltung einer Einwilligungserklärung zur künftigen Verwendung habe ich als Beratungsanfrage gewertet. Hierzu erhält der SiBe mit gesondertem Schreiben Mitteilung.

Über die vorstehenden Ausführungen hinaus möchte ich die Empfehlung aussprechen, bei der Befüllung des Freitextfeldes „Kurzbemerkung“ in der Datei SeCon Gesundheitsdaten nur sehr restriktiv zu verwenden, bestenfalls auf neutrale Bearbeitungshinweise umzustellen. Ich stimme zu, dass die Information der Gehörlosigkeit für den SiBe als Bearbeitungshinweis zur Aufgabenerfüllung erforderlich ist und somit noch von § 31 SÜG gedeckt ist. Ein neutraler Vermerk ohne Verwendung des Gesundheitsdatums (z.B. „keine telefonische Kontaktaufnahme möglich“) wäre meines Erachtens der Aufgabenerfüllung gleich zweckdienlich, dabei jedoch weniger eingriffsintensiv aus Sicht der betroffenen Person.

5. Berechnung der Vernichtungsfrist und Dokumentation des Vernichtungsdatums

In die Sicherheitsakte sind gemäß §§ 30, 18 Abs. 1 SÜG alle die Sicherheitsüberprüfung betreffenden Informationen aufzunehmen. Dies umfasst die Dokumentation aller Bearbeitungs- und Verfahrensschritte. Dazu gehören unter anderem die gemäß §§ 30, 19 Abs. 2 und 31, 22 Abs. 2 Nr. 1 SÜG tagesgenau zu berechnenden Vernichtungs- und Löschfristen.

Um das Datum der Vernichtung bestimmen zu können, muss im ersten Schritt das fristauslösende Ereignis korrekt ermittelt und dokumentiert werden. Gemäß 19 Abs. 2 SÜG beginnt die Vernichtungsfrist am Tag des Ausscheidens aus der sicherheitsempfindlichen Tätigkeit zu laufen. Maßgeblich ist nicht, wann die betroffene Person die Entmächtigung unterzeichnet. In den genannten Fällen (FL 90-96, 100) besteht das Risiko, dass die Sicherheitsakten nicht rechtzeitig vernichtet werden. Das Mitteilen eines falschen Datums des Ausscheidens an das BMWK als zuständige Stelle – im nächsten Arbeitsschritt - führt außerdem dazu, dass die dort geführte Sicherheitsakte ebenfalls nicht rechtzeitig vernichtet werden kann. In den genannten Fällen (FL 90-96, 100) sind die Veränderungsmitteilungen an das BMWK daher zu korrigieren und erneut abzusetzen. Die SeCon-Datenbank ist ebenfalls entsprechend zu korrigieren zur Korrektur des bestehenden Wiedervorlagesystems.

Bei der Vernichtung der Sicherheitsakte handelt es sich um einen weiteren anstehenden Bearbeitungsschritt. Diese Information muss sich ebenfalls unmittelbar aus der Sicherheitsakte selbst ergeben. Eine zusätzliche Dokumentation des Vernichtungsdatums in einer Datei oder eine automatisierte Berechnung und Erinnerung in einem Wiedervorlagesystem wie beispielsweise in SeCon genügen dem nicht.

Die Dokumentationspflicht gilt daher auch unabhängig von dem parallel bestehenden elektronischen Wiedervorlagesystem in SeCon.

Das zusätzlich praktizierte monatliche Ordnerverfahren des SiBe trägt dazu bei, dass monatlich eine Vernichtung der Sicherheitsakten erfolgt, was in der Praxis ein gangbarer Weg ist. Dennoch ist das taggenaue Vernichtungsdatum zu berechnen und zu notieren. Dies ist nicht nur hinsichtlich der vollständigen Dokumentationspflichten relevant, sondern auch dann, wenn die betroffene Person beispielsweise die sicherheitsempfindliche Tätigkeit innerhalb der Aufbewahrungsfrist wiederaufnimmt. Nur wenn das Vernichtungsdatum tagesgenau berechnet wurde, kann der SiBe feststellen, ob er die vorhandene Sicherheitsakte tatsächlich weiterführen darf oder ob diese hätte bereits vernichtet sein müssen, auch wenn in der Praxis nur einmal zum Monatsende vernichtet wird.

Für die aufbewahrungspflichtigen Sicherheitsakten sind die tagesgenauen Vernichtungsfristen in bzw. alternativ auf der Papierakte zu notieren.

IV. Fazit

Bei meiner Kontrolle habe ich einige Mängel bei der Gewährleistung der datenschutzrechtlichen Bestimmungen des SÜG festgestellt.

Nach Ausübung meines pflichtgemäßen Ermessens sehe ich zunächst von einer Beanstandung gemäß § 16 Abs. 2 Satz 1 BDSG ab, behalte mir diese jedoch ausdrücklich vor, wenn die festgestellten Mängel in angemessener Frist nicht beseitigt und keine Maßnahmen ergriffen werden, um vergleichbare Mängel in Zukunft zu vermeiden.

Dem liegen folgende Erwägungen zu Grunde:

Das Unternehmen zeigte sich äußerst kooperativ und signalisierte, meine Hinweise und Empfehlungen anzunehmen und künftig umzusetzen. Sämtliche aufgefundenen Mängel können durch entsprechende Schwärzungen, Ergänzungen oder technisch-organisatorische Maßnahmen unproblematisch bereinigt bzw. abgestellt werden. Hierbei handelte es sich zudem um nur wenige Ausnahmefälle. Die Personalausstattung des Bereichs personeller Geheim- und Sabotageschutzschutz ist gemessen am sehr hohen Fallaufkommen vergleichsweise gering, aber noch angemessen, was sich in der insgesamt sehr ordentlichen Führung der Sicherheitsakten zeigt und den bemerkenswerten Organisationsstrukturen in dem Arbeitsbereich zu verdanken ist. Besonders hervorzuheben ist die qualitativ hochwertige Arbeit des SiBe und seiner beiden Stellvertreter, die verdeutlicht, dass der

personelle Geheim- und Sabotageschutz einen adäquaten Stellenwert im Unternehmen hat.

Ich bitte in diesem Zusammenhang ausdrücklich um

1. Stellungnahme zu meinem Kontrollbericht innerhalb eines Monats ab Zugang dieses Kontrollberichts,

2. Beseitigung der festgestellten Mängel in den Sicherheitsakten und Datensätzen, die Gegenstand meiner Kontrolle waren, innerhalb von drei Monaten ab Zugang dieses Kontrollberichts.

3. Überprüfung aller weiteren Sicherheitsakten und aller personenbezogenen Daten in der automatisierten Datei hinsichtlich etwaiger Mängel im laufenden Geschäftsbetrieb, unter Beachtung der unter Ziff. I.1. bis I.5. aufgeführten Punkte.

V. Hinweis zur Veröffentlichung

Erlauben Sie mir abschließend noch den folgenden Hinweis:

Der BfDI strebt ein modernes Informationsmanagement zwischen Bürger/in und Staat an, das eine Begegnung auf Augenhöhe ermöglichen soll. In Verfolgung dieses Ziels werden Kontrollberichte und/oder die jeweiligen Bescheide im rechtlich zulässigen Rahmen veröffentlicht. Sofern die kontrollierte Stelle dies wünscht, wird auch deren Stellungnahme zum Kontrollbericht veröffentlicht. Die Veröffentlichung erfolgt in der Regel nach Abschluss der Kontrolle.

Sofern der Kontrollbericht bzw. die Stellungnahme der kontrollierten Stelle Namen einzelner natürlicher Personen enthalten, schwärzt der BfDI diese vor der Veröffentlichung. Das Gleiche gilt für eventuell ausgewiesene Geschäftszeichen der geprüften Akten. Die im Kontrollbericht benannte Fallliste wird ebenfalls nicht veröffentlicht. Sofern der Kontroll-bericht Informationen zur Identifikation geprüfter Unternehmen enthält, werden auch diese vor Veröffentlichung unkenntlich gemacht.

Sofern Bedenken gegen die geplante Veröffentlichung bestehen oder zusätzliche Schwärzungen für erforderlich gehalten werden, bitte ich, mir dies ggf. unter Angabe der zusätzlich zu schwärzenden Passagen innerhalb der unter Ziff. IV. genannten Frist zur Stellungnahme mitzuteilen.

Über eine eventuelle Pflicht zur Herausgabe nach den Regelungen des Informationsfreiheitsgesetzes des Bundes (IFG) ist im Einzelfall gesondert zu entscheiden.

Mit freundlichen Grüßen
im Auftrag

[redacted]