Hinweise zum Datenschutz im Sicherheitsüberprüfungsverfahren
Wie sind Sicherheitsakten in nichtöffentlichen Stellen (Unternehmen) zu führen?

(Stand: 25.04.2023)

I. Was ist Gegenstand dieses Papiers?

Gegenstand dieses Papiers sind die datenschutzrechtlichen Anforderungen an die in Papierform oder elektronisch geführten Sicherheitsakten. Es richtet sich an Sicherheitsbevollmächtigte (SiBe) bzw. Sabotageschutzbeauftragte (SaBe) in nichtöffentlichen Stellen, die Sicherheitsakten nach dem Sicherheitsüberprüfungsgesetz (SÜG) führen. Im weiteren Verlauf wird kontextabhängig nur die oder der SiBe genannt; alle Informationen gelten aber stets auch für die oder den SaBe.

Soweit im Dokument zum sprachlichen Verständnis nur Vorschriften des öffentlichen Bereichs des SÜG aufgeführt werden, sind diese über Verweisungen oder mangels einschlägiger Sonderregelungen für den nichtöffentlichen Bereich anwendbar.

II. Was ist eine Sicherheitsakte und wozu dient sie?

In der Sicherheitsakte befinden sich alle Informationen zum Sicherheitsüberprüfungsverfahren einer betroffenen Person, die für die Sicherheitsüberprüfung erforderlich sind und den aktuellen Verfahrensstand abbilden sollen. Jede Sicherheitsüberprüfung verarbeitet personenbezogene Daten und greift dadurch in das informationelle Selbstbestimmungsrecht ein. Als entsprechende Rechtsgrundlage regelt deshalb das SÜG aus datenschutzrechtlicher Sicht, welche Informationen zur Sicherheitsakte genommen werden dürfen.

III. Welche gesetzlichen Regelungen gelten somit?

1. Wer führt die Sicherheitsakte?

Im nichtöffentlichen Bereich existieren für jede betroffene Person zwei Sicherheitsakten. Eine Sicherheitsakte wird durch den SiBe im Unternehmen geführt und eine weitere bei der jeweils zuständigen öffentlichen Stelle.

Für das Unternehmen ergibt sich diese Verpflichtung aus **§ 30 i. V. m. § 18 Abs. 1 SÜG** und erfolgt gem. § 25 Abs. 3 SÜG durch die oder den SiBe bzw. die oder den SaBe. Die zuständige Stelle führt gem. § 25

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL referat36@bfdi.bund.de
INTERNET www.datenschutz.bund.de

Abs. 1 und Abs. 2 i. V. m. § 18 Abs. 1 SÜG eine eigene weitere Sicherheitsakte. Im Bereich des Geheimschutzes ist nach **§ 25 Abs. 1 SÜG** das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) die zuständige Stelle, soweit gesetzlich nichts anderes bestimmt ist und keine andere Bundesbehörde diese Aufgabe vom BMWK übernommen hat. Im Bereich des Sabotageschutzes richtet sich die Zuständigkeit nach **§ 25 Abs. 2 i. V. m. § 34 SÜG**.

Die Sicherheitsakte der oder des Betroffenen ist nicht Teil der Personalakte **(§ 18 Abs. 3 Satz 1 und 2 SÜG)** und muss gesondert geführt und aufbewahrt werden **(§ 19 Abs. 1 SÜG)**. Die Sicherheitsakte darf weder der personalverwaltenden Stelle noch der betroffenen Person zugänglich gemacht werden. Nur ausnahmsweise ist unter den in **§ 23 Abs. 6 SÜG** geregelten Voraussetzungen eine Einsichtnahme in die eigene Sicherheitsakte möglich. Daher dürfen auch die oder der SiBe sowie Mitarbeitende, die mit der Bearbeitung von Sicherheitsakten betraut sind, nicht auf ihre eigene Sicherheitsakte zugreifen und keinesfalls ihr eigenes Überprüfungsverfahren bearbeiten. Denn das würde die Einsichtnahme in die eigene Sicherheitsakte ermöglichen und wäre als Verstoß gegen § 18 Abs. 3 Satz 2 SÜG zu werten. Lediglich im Ausnahmefall, wenn und solange die Geheimschutzorganisation nicht mehr gewährleistet werden kann, ist es vertretbar, wenn der oder die SiBe bzw. die Stellvertretung hierauf vorübergehend Zugriff haben. Dies wäre beispielsweise der Fall, wenn die Nachbesetzung der oder des SiBe bzw. dessen Vertretung nicht zeitnah erfolgen kann und weitere Geheimschutzmitarbeitende aufgrund der Unternehmensgröße nicht zur Verfügung stehen.

Die Sicherheitsakte verbleibt bei einem Wechsel des Betroffenem zu einem neuen Arbeitgeber bis zur anstehenden Vernichtung beim ursprünglichen Arbeitgeber **(§ 30 SÜG)**.

2. In welcher Form ist die Sicherheitsakte zu führen?

Die Sicherheitsakte kann wahlweise in Papierform oder elektronisch geführt werden **(§ 18 Abs. 6 SÜG)**. Jedoch muss sich die aktenführende Stelle festlegen und die entsprechende Akte vollständig in der gewählten Art führen.

Eine Mischform ist nicht zulässig; insbesondere darf der Aktenkontext nicht zersplittert oder aufgelöst werden. Ergibt sich eine vollständige Sicherheitsakte erst aus allen digitalen und analogen Dokumenten zusammen, ist dies unzulässig. Entscheidend ist, dass die oder der SiBe das Sicherheitsüberprüfungs-verfahren vollständig in einer einheitlichen Akte erfasst.

Eine doppelte Aktenführung ist ebenfalls unzulässig.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL referat36@bfdi.bund.de
INTERNET www.datenschutz.bund.de

Allerdings dürfen manche Dokumente nicht digitalisiert werden oder sind im Original (z.B. Ermächtigungsurkunde des BMWK) aufzubewahren. Bei elektronischer Aktenführung muss deshalb eine Papierrestakte weitergeführt werden.[1] Eine elektronische Akte ist dann erst mit einem entsprechenden Verweis vollständig, durch den sich das Original schnell finden lässt.

Im nichtöffentlichen Bereich ist es zulässig, jenseits der Aktenführung nach **§ 31 Satz 1 SÜG** personenbezogene Daten in einer automatisierten Datei zu speichern, soweit dies zur Aufgabenerfüllung erforderlich ist. Dies erlaubt auch die zusätzliche elektronische Speicherung einzelner Dokumente neben der Papierakte soweit sie zur Aufgabenerfüllung erforderlich sind. Die Sicherheitsakte darf dadurch aber nicht vollständig kopiert werden. Zudem muss die Papierakte weiterhin vollständig sein. Es gilt zu beachten, das personenbezogene Daten zu einer mitbetroffenen Person nicht dieser Speichererlaubnis unterliegen. Sie dürfen nicht elektronisch verarbeitet werden.

3. Was bedeutet das in der Praxis?

Bei Papierakten: Dokumente, die elektronisch erstellt und versandt werden, müssen ausgedruckt und zur Akte genommen werden, um eine vollständige Sicherheitsakte zu gewährleisten. Der elektronische Schriftverkehr ist in der Regel zu löschen. Ausnahmen sind gem. § 31 Satz 1 SÜG möglich (siehe vorherige Ausführungen).

Bei Umstellung von Papierakten auf elektronische Aktenführung[2]: Nach der Digitalisierung ist eine vorherige Papierakte zu vernichten. Davon ausgenommen sind Dokumente, die – wie oben dargestellt –im Original aufzubewahren sind. Für diese Unterlagen ist eine Papierrestakte anzulegen, weiterhin muss die elektronische Akte auf die jeweiligen Originale verweisen.

Bei elektronischer Aktenführung: Falls erforderlich, ist zusätzlich eine Papierrestakte mit Originaldokumenten zu führen (siehe vorherige Ausführungen). In der elektronischen Akte ist auch hier zu kennzeichnen, welche Originaldokumente in Papierform aufbewahrt werden.

[1] Dies betrifft nur Dokumente, die zwingend im Original vorzuhalten sind bzw. nicht digitalisiert werden dürfen.
[2] Es ist möglich, einzelne Sicherheitsakten in Papierform weiterzuführen. Der Aktenbestand insgesamt kann sowohl aus Papierakten als auch aus elektronischen Sicherheitsakten bestehen. Es gilt zu beachten, dass die jeweilige Sicherheitsakte einer Person in ihrer Gesamtheit vollständig ist und entweder in Papierform oder elektronisch vorgehalten wird.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL referat36@bfdi.bund.de
INTERNET www.datenschutz.bund.de

4. Welche Inhalte dürfen in die Sicherheitsakte?

Grundsätzlich gehören nur rechtmäßig erhobene Daten in die Sicherheitsakte. Datenerhebungen bei der betroffenen Person und bei anderen Stellen sind nur zulässig, um Aufgaben nach dem SÜG zu erfüllen (**vgl. §§ 11 f. SÜG**). Welche Daten zur betroffenen oder mitbetroffenen Person sowie zu ggf. weiteren Personen erhoben und somit in der Sicherheitsakte aufgenommen werden dürfen, ist über die Verweisung des § 30 SÜG geregelt in **§§ 13, 15a, 17 und 18 SÜG**.

Gem. **§ 18 Abs. 1 SÜG** sind in die Sicherheitsakte alle die Sicherheitsüberprüfung unmittelbar betreffenden Informationen aufzunehmen. Dazu gehören typischerweise folgende Unterlagen:

- Antrag der Fachabteilung / Einsatzleitung oder Personalstelle zur Sicherheitsüberprüfung aus dem hervorgeht, dass für die vorgesehene Tätigkeit eine Sicherheitsüberprüfung erforderlich ist,
- Antrag der oder des SiBe zur Durchführung einer Sicherheitsüberprüfung bei der zuständigen Stelle (Geheimschutz: Antrag auf VS- Ermächtigung, Anlage 19a GHB; Sabotageschutz: Formular zur Überprüfung im Bereich Sabotageschutz, Formular vpS08),
- Geheimschutz: Sicherheitserklärung mit Lichtbild[3] und ggf. Anlagen[4], ggf. Antrag an den BStU[5] (Kopie aller Unterlagen, die in diesem Zusammenhang an das BMWK mit der Anlage 19a GHB übermittelt werden.)
- Sabotageschutz: Sicherheitserklärung mit Lichtbild[6] (Kopie aller Unterlagen, die in diesem Zusammenhang an das BMWK mit dem Antrag auf eine Sabotageschutzüberprüfung übermittelt werden)
- Ergebnis der Sicherheitsüberprüfung der zuständigen Stelle (Anschreiben des BMWK),
- ggf. Vermerk über Zeitpunkt und Ergebnis der Einsichtnahme in die Personalakte,
- ggf. Vermerke über Sicherheitsgespräche mit der betroffenen Person,
- ggf. Hinweise auf sicherheitserhebliche Erkenntnisse, z. B. durch Vorgesetzte oder Kollegen und Kolleginnen der betroffenen Person,
- ggf. Unterlagen über etwaige Aktualisierungs- Wiederholungsüberprüfungen, einschließlich abgegebene Sicherheitserklärungen und Anträge an die zuständige Stelle (Geheimschutz: Antrag

[3] Seit der SÜG-Änderung vom 5. Juli 2021 ist das Lichtbild in der Sicherheitserklärung wieder verpflichtend.
[4] Anlagen zur Sicherheitserklärung müssen als solche erkennbar sein (z.B. durch das Zusammenführen von Sicherheitserklärung und Anlagen mittels Büroklammer, in getackerter Form oder durch Verweis auf Anlagen in der Sicherheitserklärung selbst).
[5] Seit 17. Juni 2021 Stasi-Unterlagen-Archiv als Teil des Bundesarchivs.
[6] Seit der SÜG-Änderung vom 5. Juli 2021 ist das Lichtbild in der Sicherheitserklärung wieder verpflichtend.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL referat36@bfdi.bund.de
53117 Bonn INTERNET www.datenschutz.bund.de

auf VS- Ermächtigung, Anlage 19a GHB, ggf. Antrag an den BStU[7]; Sabotageschutz: Formulare S01 vpS und S02 vpS),

- Nachweis, dass die betroffene Person eine sicherheitsempfindliche Tätigkeit ausübt (Geheimschutz: Ermächtigungs- oder Zulassungsurkunde, Kopie Ermächtigungsbestätigung, ggf. SiBe-Bescheinigungen; Belehrungsbestätigung; Sabotageschutz: z.B. Formular S07 vpS),
- ggf. Unterrichtungen an die zuständige Stelle nach Abschluss der Sicherheitsüberprüfung oder Beendigung der sicherheitsempfindlichen Tätigkeit (Geheimschutz: Veränderungsmeldungen - Anlage 15 GHB, Erklärung beim Erlöschen der Ermächtigung zum Zugang zu Verschlusssachen – Anlage 14 GHB; Sabotageschutz: Veränderungsmitteilung Formular S19 vpS),
- ggf. Einverständnis zur Weiterleitung personenbezogener Daten im Rahmen des Besuchskontrollverfahrens (Geheimschutz: Anlage 19h GHB; Sabotageschutz: Erklärung zur Einwilligung der Datenweitergabe),
- ggf. Zusatzvereinbarung zum Arbeitsvertrag,
- ggf. Belehrungsnachweise,
- und Vermerke und Wiedervorlagen zur Bearbeitung der Sicherheitsakte.

§ 18 Abs. 2 Satz 1 SÜG gilt erst, wenn eine sicherheitsempfindliche Tätigkeit tatsächlich aufgenommen wurde. In die Sicherheitsakte sind dann auch zusätzliche Informationen über die persönlichen, dienstlichen und arbeitsrechtlichen Verhältnisse der Personen, die mit einer sicherheitsempfindlichen Tätigkeit befasst sind, aufzunehmen, soweit sie für die sicherheitsmäßige Beurteilung erheblich sind.

§ 18 Abs. 2 Satz 2 SÜG konkretisiert dies durch eine beispielhafte, jedoch nicht abschließende Aufzählung von Informationen, die – sofern erheblich – in die Sicherheitsakte aufzunehmen sind. Dazu gehören folgende Unterlagen:

- Zuweisung, Übertragung einer sicherheitsempfindlichen Tätigkeit, die dazu erteilte Ermächtigung sowie deren Änderungen und Beendigung,
- Umsetzung und Ausscheiden,
- Änderungen des Namens, eines Wohnsitzes und der Staatsangehörigkeit,
- Beginn oder Ende einer Ehe, einer Lebenspartnerschaft oder einer auf Dauer angelegten Gemeinschaft,

[7] Seit 17. Juni 2021 Stasi-Unterlagen-Archiv als Teil des Bundesarchivs.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL referat36@bfdi.bund.de
INTERNET www.datenschutz.bund.de

- Anhaltspunkte für Überschuldung, insbesondere Pfändungs- und Überweisungsbeschlüsse, Mitteilungen über abgeschlossene Insolvenzverfahren sowie Beschlüsse zur Eröffnung eines Insolvenzverfahrens und zur Restschuldbefreiung sowie
- Strafverfahren und Disziplinarsachen, sowie dienst- und arbeitsrechtliche Maßnahmen.

Die Aktenführung der nichtöffentlichen Stelle ist in **§ 30 SÜG** geregelt, der hinsichtlich der inhaltlichen Anforderungen auf **§ 18 Abs. 1 und 2 SÜG** verweist. Abweichungen ergeben sich durch die nach **§ 25 Abs. 1 und 3 SÜG** unterschiedlich zugewiesenen Aufgaben zwischen BMWK als zuständiger Stelle und der oder dem SiBe der nichtöffentlichen Stelle. Dies führt dazu, dass die Sicherheitsakte des Unternehmens gerade keine Kopie der Sicherheitsakte beim BMWK ist.

Die nichtöffentliche Stelle nimmt nach **§ 26 SÜG** die Sicherheitserklärung der betroffenen Person entgegen, prüft die Vollständigkeit und Richtigkeit der Angaben, gibt die Sicherheitserklärung an die zuständige Stelle (BMWK) weiter und teilt dieser ggf. vorhandene sicherheitserhebliche Erkenntnisse mit. Außerdem hat das Unternehmen nach **§ 27 Satz 4 SÜG** eine Nachberichtspflicht und muss das BMWK unverzüglich unterrichten, wenn sicherheitserhebliche Erkenntnisse über die betroffene Person oder die mitbetroffene Person bekanntwerden.

Ein Unterschied beim zulässigen Akteninhalt ergibt sich bei den oben beschriebenen Informationen über die persönlichen, dienstlichen und arbeitsrechtlichen Verhältnisse im Sinne des **§ 18 Abs. 2 SÜG**. Hier hat die oder der SiBe zu prüfen, ob diese erforderlich sind, um die Aufgaben des SÜG und dabei insbesondere die Nachberichtspflichten erfüllen zu können. Hierfür bedarf es – wie unten noch erläutert wird – stets einer Betrachtung im Einzelfall.

Bei Dokumenten oder Informationen, die von der zuständigen Stelle angefordert werden, muss die oder der SiBe beurteilen, ob sie für die eigenen Aufgaben erheblich sind. Ist dies der Fall, können die Unterlagen in der Sicherheitsakte des Unternehmens aufgenommen werden. Auch bei Dokumenten oder Informationen, die von der betroffenen Person freiwillig vorgelegt und damit von ihr selbst als verfahrensfördernd angesehen werden, ist zu prüfen, ob sie sicherheitserheblich sind. Beim Verakten ist unbedingt darauf zu achten, dass personenbezogene Daten Dritter dauerhaft unkenntlich zu machen sind.

Herkunft, Sachzusammenhang und Erforderlichkeit personenbezogener Informationen müssen nachvollziehbar dokumentiert sein (siehe hierzu weitere Hinweise unter Ziff. IV.1).

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL referat36@bfdi.bund.de
INTERNET www.datenschutz.bund.de

§ 15a i.V.m. § 29 SÜG konkretisiert, welche Informationen zur betroffenen Person die personalverwaltende Stelle an die oder den SiBe weitergeben muss. Diese Daten sind auch in der Sicherheitsakte aufzunehmen. Dazu zählen u.a. folgende Informationen:

- Ausscheiden aus der sicherheitsempfindlichen Tätigkeit oder Bekanntwerden der Nichtaufnahme der sicherheitsempfindlichen Tätigkeit,
- Tätigkeitswechsel (Umsetzung, neues Projekt o.ä.),
- Namensänderungen, Änderungen des Wohnsitzes, Änderung der Staatsbürgerschaft, Personenstandsänderung (Änderung des Geschlechtseintrages),
- im Geheimschutz: Änderungen in finanziellen Angelegenheiten (Anhaltspunkte für Überschuldung, insbesondere Pfändungs- und Überweisungsbeschlüsse, Insolvenzverfahren),
- Strafverfahren und arbeitsrechtliche Maßnahmen,
- im Geheimschutz: Nebentätigkeiten,
- sonstige Erkenntnisse, die sicherheitserheblich sein können.

Weitere Hinweise hierzu gibt **die Allgemeine Verwaltungsvorschrift zum personellen Geheimschutz und zum vorbeugenden personellen Sabotageschutz – SÜG-Ausführungsvorschrift (SÜG-AVV) zu § 15a**. Die AVV ist für nichtöffentliche Stellen zwar nicht unmittelbar anwendbar, kann jedoch zur Auslegung mit herangezogen werden.

Der § 15a SÜG gilt über § 29 Abs. 2 SÜG auch im nichtöffentlichen Bereich, allerdings übernimmt hier das Unternehmen diese Aufgabe. Die oben genannten Informationen sind also von der personalverwaltenden Stelle des Unternehmens an die oder den SiBe zu übermitteln, wo die Informationen veraktet und an das BMWK oder ggf. eine andere zuständige Stelle weitergeleitet werden.

5. Wann dürfen Informationen aus der Sicherheitsakte an andere Stellen übermittelt werden?

Hier besteht eine enge Zweckbindung: Das Unternehmen darf personenbezogene Daten aus der Sicherheitsüberprüfung grundsätzlich nur an die zuständige Stelle (BMWK) übermitteln. Welche Informationen das sind, ist in den **§§ 26 bis 29 SÜG** abschließend geregelt. Dazu gehören u.a. Daten aus der Sicherheitserklärung, die Mitteilung sicherheitserheblicher Erkenntnisse und Meldungen, dass sich persönliche und arbeitsrechtliche Verhältnisse geändert haben.

Innerhalb des Unternehmens darf die oder der SiBe solche Daten nur teilen, wenn dies für die Sicherheitsüberprüfung erforderlich ist. Das kann nach **§ 27 Satz 2 SÜG** beispielsweise der Fall sein, wenn

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL referat36@bfdi.bund.de
53117 Bonn INTERNET www.datenschutz.bund.de

sicherheitserhebliche Erkenntnisse auftreten, die der oder die SiBe beobachten soll. Diese Daten dürfen dann intern verarbeitet und ggf. übermittelt werden. Die Personalabteilung darf die Informationen jedoch nur erhalten, wenn es für die Aufgabenerfüllung nach dem SÜG zwingend erforderlich ist. Das gilt regelmäßig nicht für Details zu sicherheitserheblichen Erkenntnissen.

Darüber hinaus kann im Ausnahmefall auch ein direkter Datenaustausch zwischen Unternehmen und BfV zulässig sein. Erfahrungsgemäß dann, wenn das BfV in seiner Funktion als mitwirkende Behörde im Sicherheitsüberprüfungsverfahren bei der betroffenen Person selbst Dokumente zur Vorlage anfragt und diese die Unterlagen nicht persönlich, sondern über den oder die SiBe weiterleitet.[8]

IV. Weitere Hinweise für die Praxis

Aus datenschutzrechtlicher Sicht ergeben sich insbesondere folgende Anforderungen an die Aktenführung der Sicherheitsakten:

1. Dokumentation zu Herkunft, Übermittlungswegen und Verarbeitungszwecken

Im SÜG ist klar geregelt, dass die erhobenen Daten dem Zweck der jeweils individuellen Sicherheitsüberprüfung dienen müssen (§ 11 SÜG). Der Sicherheitsakte muss jederzeit entnommen werden können, woher bestimmte Informationen zur betroffenen oder mitbetroffenen Person stammen und weshalb sie aufbewahrt werden. Ansonsten ist nicht nachvollziehbar, ob diese Daten tatsächlich für die Aufgaben nach dem SÜG erforderlich sind. Es empfiehlt sich daher, auch mündlich besprochene Vorgänge in der Sicherheitsakte zu dokumentieren. Da § 21 SÜG die erhobenen Daten einer strengen Zweckbindung unterwirft, muss in der Sicherheitsakte weiterhin stets erkennbar sein, an welche dritten Stellen und zu welchem Zweck die Informationen übermittelt wurden.

2. Umgang mit Daten unbeteiligter Dritter

Personenbezogene Daten unbeteiligter Dritter dürfen in der Sicherheitsakte nicht verarbeitet werden, da hierfür eine Rechtsgrundlage fehlt. Darunter fallen alle Daten, die nicht der betroffenen, mitbetroffenen oder anderen verfahrensbeteiligten Personen zugeordnet werden können und für das vorliegende Sicherheitsüberprüfungsverfahren entbehrlich sind. Es dürfen folglich nur solche Daten Dritter erhoben werden, für die eine Rechtsgrundlage existiert. In der Praxis kommt es immer wieder vor, dass in der

[8] In diesem Fall sollte seitens des oder der SiBe eine Weiterleitung dieser Dokumente postalisch oder auf elektronischem Wege verschlüsselt an das BfV erfolgen. Weiterhin sollten in solchen Fällen Herkunft und Sachzusammenhang in der Sicherheitsakte nachvollziehbar dokumentiert sein.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL referat36@bfdi.bund.de
53117 Bonn INTERNET www.datenschutz.bund.de

Sicherheitserklärung unzulässige Daten erhoben werden. Es gilt daher insbesondere im Rahmen der Prüfung der Vollständigkeit und Richtigkeit der Angaben in der Sicherheitserklärung, je nach Art der Sicherheitsüberprüfung, folgendes zu beachten:

- Liegt eine Trennung oder Scheidung bei der betroffenen Person vor, sind keine Angaben zu Ehegatten/Lebenspartnern/ Lebensgefährten zu machen. Ggf. sind personenbezogene Daten zu einem neuen Lebenspartner/Lebensgefährte anzugeben. Bei einer auf Dauer angelegten Gemeinschaft/einer noch nicht rechtskräftig geschiedenen Ehe oder Lebenspartnerschaft sind die besonderen Ausfüllhinweise zur Sicherheitserklärung unter Punkt 1.1 Familienstand und Punkt 2. zu beachten. In diesen Fällen muss eine Zustimmung der ehemaligen mitbetroffenen Person zur Angabe seiner/ihrer personenbezogenen Daten in der aktuellen Sicherheitserklärung erfolgen. Eine Einbeziehung in die aktuelle Sicherheitsüberprüfung erfolgt hingegen nicht mehr (es werden keine Maßnahmen gem. § 12 SÜG durchgeführt).
- Kinder und Personen (z.B. Mitbewohner), die mit im Haushalt der betroffenen Person leben, sind nur in der Sicherheitserklärung anzugeben, wenn diese über 18 Jahre alt sind.
- Bei einer erweiterten Sicherheitsüberprüfung (Ü 2) dürfen keine Referenzpersonen angegeben werden.
- Hat ggf. die mitbetroffene Person per Unterschrift Ihre Zustimmung zur Verarbeitung Ihrer Daten gegeben?

Werden im Rahmen einer Aktualisierungsüberprüfung die Angaben in der ursprünglichen Sicherheitserklärung (altes Formular) aktualisiert, bleiben seinerzeit rechtmäßig erhobene Daten Bestandteil der Sicherheitserklärung und sind nicht unkenntlich zu machen. Sollten sich zwischenzeitlich Änderungen ergeben haben, sind diese durch den Betroffenen z.B. durch Streichung oder Ergänzung kenntlich zu machen.

Praxisbeispiele:

Ändert sich etwas am Familienstand, dann sind bei der Aktualisierung die in der ursprünglichen Sicherheitserklärung rechtmäßig erhobenen personenbezogenen Daten zum Ehegatten/Lebenspartnern/Lebensgefährten durchzustreichen.

Fallen im Haushalt lebende Personen über 18 Jahre bei der Aktualisierung der Sicherheitserklärung weg, sind diese ebenfalls durchzustreichen. Sind hingegen zusätzliche Angaben zu im Haushalt lebenden

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL referat36@bfdi.bund.de
53117 Bonn INTERNET www.datenschutz.bund.de

Kindern zu machen, da diese zwischenzeitlich über 18 Jahre alt sind, werden die Angaben in der ursprünglichen Sicherheitserklärung ergänzt.

Wenn es sich nicht vermeiden lässt, Dokumente mit personenbezogenen Daten unbeteiligter Dritter zur Sicherheitsakte zu nehmen, dann sind diese Drittdaten dauerhaft unkenntlich zu machen. In der Praxis handelt es sich dabei häufig um Sammelmeldungen der Personalstelle. In solchen Fällen sind auch Daten von Mitarbeitenden zu schwärzen, die nicht am konkreten Sicherheitsüberprüfungsverfahren beteiligt sind.

Ebenfalls unzulässig sind Daten, die im Rahmen des SÜG generell nicht erhoben werden dürfen (z.B. Angaben zur Religionszugehörigkeit, personenbezogene Daten Minderjähriger).

Für die Praxis empfiehlt sich folgendes Vorgehen:

Sollten zusätzliche Dokumente zur Sicherheitsakte genommen werden, ist zu prüfen, ob diese Daten von Dritten enthalten. Solche Daten sind unkenntlich zu machen, wenn sie für die Sicherheitsüberprüfung nicht erforderlich sind. Erforderlich ist beispielsweise bei amtlichen Dokumenten, wer das Dokument erstellt hat und an wen es adressiert ist (Amtspersonen, Urheber, Adressaten). Bei Insolvenzverfahren sind die Verwalterin bzw. der Verwalter relevant, aber nicht immer, wem die betroffene Person etwas schuldet. Bei Scheidungsbeschlüssen dürfen Informationen über den zu zahlenden Unterhalt in der Sicherheitsakte aufgenommen werden, personenbezogene Daten der Kinder aber regelmäßig nicht.

3. Umgang mit Informationen, die für die sicherheitsmäßige Beurteilung erheblich sind

§ 18 Abs. 2 Satz 2 SÜG regelt die zulässigen Inhalte der Sicherheitsakte nicht abschließend, sondern eröffnet einen Beurteilungsspielraum. Dieser ist dadurch begrenzt, dass die betreffenden Unterlagen gem. § 18 Abs. 2 Satz 1 SÜG für die sicherheitsmäßige Beurteilung erheblich sein müssen. Dies ist der Fall, wenn sie für eine nachvollziehbare Dokumentation der sicherheitsmäßigen Bewertung erforderlich sind.

Für das Verakten von Dokumenten, die sich von den in § 18 Abs. 2 Satz 2 SÜG genannten Beispielen unterscheiden, gilt grundsätzlich:

Dokumente dürfen in die Sicherheitsakte aufgenommen werden, wenn sie für die Aufgabenerfüllung nach dem SÜG notwendig sind. Das ist der Fall, wenn die Informationen erforderlich sind, um sicherheitserhebliche Erkenntnisse zu bewerten. Der zuständigen Stelle und auch der oder dem SiBe im Unternehmen steht hier ein Beurteilungsspielraum zu, der im Einzelfall zu klären ist. Aus

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL referat36@bfdi.bund.de
INTERNET www.datenschutz.bund.de

datenschutzrechtlicher Sicht ist entscheidend, dass die Aufnahme des entsprechenden Dokumentes oder des personenbezogenen Datums nachvollziehbar ist. Ergibt sich diese Nachvollziehbarkeit nicht aus dem Sachverhalt an sich, sollte dies in der Sicherheitsakte dokumentiert werden. Das kann ein Vermerk oder eine Notiz sein, die begründet, weshalb das Dokument in die Sicherheitsakte aufgenommen wurde.

Einer zusätzlichen Dokumentation bedarf es auch dann nicht, wenn aus internen Handlungsanweisungen oder sonstigen schriftlichen Vorgaben hervorgeht, welche Unterlagen in der sicherheitsmäßigen Überprüfung verwendet werden.

Es gilt zu beachten, dass Informationen oder Dokumente nicht allein deswegen erforderlich sind, weil sie von der betroffenen Person selbst oder von der Personalabteilung übermittelt werden. Die Erforderlichkeit der Veraktung ist im Einzelfall festzustellen. Eingereichte, aber nicht erforderliche (z.B. offensichtlich sachfremde) Unterlagen sind an die betroffene Person zurückzugeben oder zu vernichten bzw. zu löschen.

In die Sicherheitsakte gehören grundsätzlich keine Unterlagen, die typischerweise zur Personalakte gehören. Eine Ausnahme stellt eine Zusatzvereinbarung zum Arbeitsvertrag dar, die aufgrund der Aufnahme der sicherheitsempfindlichen Tätigkeit geschlossen wurde. Diese dokumentiert die Aufnahme der sicherheitsempfindlichen Tätigkeit und es bestehen aus datenschutzrechtlicher Sicht keine Bedenken diese zur Sicherheitsakte zu nehmen (vgl. Anlage 38 GHB). Insbesondere weil diese in der Praxis bei Unternehmen nicht immer zur Personalakte genommen werden. Die übrigen Informationen können – sofern sie nötig sind – über das Einsichtsrecht in die Personalakte gem. § 13 Abs. 6 Satz 2 und 3 SÜG vorübergehend beigezogen werden. Sollte dennoch ausnahmsweise ein Verakten erforderlich sein, sind alle personenbezogenen Daten, die nicht erhoben werden dürfen, unkenntlich zu machen. Die Begründung ist zu dokumentieren, wenn Sie sich nicht aus dem Dokument selbst oder weiterer Dokumente ergibt.

Die Veraktung von Personal- oder Reisepasskopien kann gerechtfertigt sein, wenn die betroffene Person in der Sicherheitserklärung ihre Staatsangehörigkeit (auch frühere) oder die einer mitbetroffenen Person nachweisen muss und die Dokumentation in der Sicherheitsakte dadurch sicherheitsrelevant und verfahrenserheblich ist. Eine Veraktung der Reisepasskopie kann auch dann gerechtfertigt sein, wenn die betroffene oder mitbetroffene Person Reisen in Staaten mit besonderen Sicherheitsrisiken (Staatenliste i. S. v. § 13 Abs. 1 Nr. 17 SÜG) nachweisen möchte. Ausweis- und Reisepasskopien dürfen als Anhang oder Ergänzung zur Sicherheitserklärung auch an die zuständige Behörde übermittelt werden. Die Regelungen

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL referat36@bfdi.bund.de
INTERNET www.datenschutz.bund.de

des SÜG gehen insoweit als spezialgesetzliche Regelungen den allgemeinen Übermittlungsverboten nach § 20 Abs. 2 Satz 2 Personalausweisgesetz und § 18 Abs. 3 Satz 2 Passgesetz vor.[9]

4. Wiedervorlagesystem und Dokumentation von Bearbeitungs- und Verfahrensschritten

Gemäß § 36 Abs. 1 Nr. 2 SÜG i.V.m. § 64 BDSG ist die verantwortliche Stelle verpflichtet, technisch-organisatorische Maßnahmen zu ergreifen, um ein risikoangemessenes Schutzniveau zu gewährleisten. Dies gilt insbesondere auch zur Gewährleistung von Lösch- und Vernichtungsfristen. Hier ist in der Regel ein Wiedervorlagesystem geboten, um den Stand der Sicherheitsüberprüfung zu überwachen und an offene Aufgaben zu erinnern. Nur so kann die oder der SiBe die einzelnen Schritte der Sicherheits-überprüfung fristgerecht bearbeiten und regelmäßig prüfen, ob personenbezogene Daten noch erforderlich sind oder bereits die Vernichtungsfristen des § 19 Abs. 2 SÜG laufen.

Das Wiedervorlagemanagement kann in der Sicherheitsakte oder (zusätzlich) elektronisch durch eine Datenbank oder Tabelle erfolgen. In der Sicherheitsakte selbst muss hinsichtlich der Vernichtung der Sicherheitsakte jedoch mindestens das fristauslösende Ereignis und das errechnete Vernichtungsdatum dokumentiert sein, weil diese sonst unvollständig ist und die wesentlichen Verfahrensschritte entgegen § 18 Abs. 1 SÜG nicht nachvollzogen werden können. Die Vernichtungsfrist ist tagesgenau zu berechnen.

Bearbeitungs- und Verfahrensschritte sind nur vollständig dokumentiert, wenn sie den Verfasser bzw. die Verfasserin und das Erstellungsdatum erkennen lassen. Dafür ist mindestens ein Namenskürzel notwendig. Das Gleiche gilt, wenn Angaben in der Sicherheitserklärung und/oder -akte (handschriftlich) ergänzt oder korrigiert werden. Auch hier muss erkennbar dokumentiert sein, wann und durch wen die Korrektur vorgenommen wurde und woher die Informationen stammen.

Bei der Sicherheitserklärung ist allerdings Folgendes zu beachten: Die Sicherheitserklärung ist gem. § 13 Abs. 6 SÜG von der betroffenen Person selbst auszufüllen. Das gilt regelmäßig auch für Änderungen oder Ergänzungen. Ausnahmsweise ist (wie im Verfahren bei öffentlichen Stellen nach der SÜG-AVV zu § 13 Abs. 6 SÜG, Ziff. 1.1) im Einzelfall eine handschriftliche Ergänzung der Sicherheitserklärung durch den/die SiBe möglich. Der Grund der Ergänzung ist jedoch in einem Vermerk zur Akte zu nehmen. Es ist darauf zu

[9] Vgl. Gesetzesbegründung zu § 20 Abs. 2 PAuswG-E, BT-Drs.787/16

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL referat36@bfdi.bund.de
53117 Bonn INTERNET www.datenschutz.bund.de

achten, dass es beim Eingreifen der/s Bearbeiterin/s selbst nur im Ausnahmefall um Ergänzungen gehen kann, welche durch einen Vermerk über die Rücksprache mit der betroffenen Person belegt sein müssen.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL referat36@bfdi.bund.de
INTERNET www.datenschutz.bund.de