Hinweise zum Datenschutz im Sicherheitsüberprüfungsverfahren
Wie sind Sicherheitsakten in öffentlichen Stellen (Behörden) 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 Geheimschutzbeauftragte (GSB) bzw. Sabotageschutzbeauftragte (SaBe) bei öffentlichen Stellen, die Sicherheitsakten nach dem Sicherheitsüberprüfungsgesetz (SÜG) führen. Im weiteren Verlauf wird kontextabhängig nur die oder der GSB genannt; alle Informationen gelten aber stets auch für die oder den SaBe. Nicht behandelt werden Sonderregelungen im Geschäftsbereich des Bundesministeriums der Verteidigung und im Bereich der Nachrichtendienste; das gilt insbesondere für die Sicherheitsüberprüfungsakte.

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. Das SÜG konkretisiert damit den Grundsatz der ordnungsgemäßen Aktenführung für öffentliche Stellen.

III. Welche gesetzlichen Regelungen gelten somit?

1. Wer führt die Sicherheitsakte?

§ 18 Abs. 1 SÜG regelt für den öffentlichen Bereich, dass die jeweilige Behörde als zuständige Stelle eine Sicherheitsakte führt. Diese Aufgabe übernimmt nach § 3a Abs. 1 SÜG die oder der jeweilige GSB bzw. nach § 3a Abs. 2 SÜG die oder der SaBe.

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

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

eigene Sicherheitsakte möglich. Daher dürfen auch die oder der GSB 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.

Wenn die betroffene Person ihre Dienststelle wechselt, aber weiterhin in einer sicherheitsempfindlichen Tätigkeit arbeitet, ist die Sicherheitsakte an den neuen Dienstherrn bzw. an die neue Dienststelle zu übergeben, § 18 Abs. 3 Satz 3 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 einzelne Akte entsprechend 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 GSB das Sicherheitsüberprüfungs-verfahren vollständig in einer einheitlichen Akte erfasst.

Eine doppelte Aktenführung ist ebenfalls unzulässig.

Allerdings dürfen manche Dokumente nicht digitalisiert werden oder sind im Original aufzubewahren (z.B. die Zustimmung zur Durchführung einer Sicherheitsüberprüfung in der Sicherheitserklärung durch die erforderliche Unterschrift). 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.

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 zu löschen.

[1] Dies betrifft nur Dokumente, die zwingend im Original vorzuhalten sind bzw. nicht digitalisiert werden dürfen.

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

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.

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, regeln die **§§ 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 oder Personalstelle zur Sicherheitsüberprüfung, aus dem hervorgeht, dass für die vorgesehene Tätigkeit eine Sicherheitsüberprüfung erforderlich ist,
- Sicherheitserklärung mit Lichtbild[3] und ggf. Anlagen[4],
- Antrag der zuständigen Stelle auf Durchführung einer Sicherheitsüberprüfung an die mitwirkende Behörde,
- Geheimschutz: ggf. Antrag der zuständigen Stelle an den BStU[5] und dessen Ergebnis,
- Ergebnis der Sicherheitsüberprüfung einschließlich sicherheitserheblicher Erkenntnisse und Erkenntnisse über ein Sicherheitsrisiko (Votum der mitwirkenden Behörde),

[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.
[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.

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

- ggf. Vermerke über Sicherheitsgespräche/Anhörungen mit der betroffenen und/oder mitbetroffenen Person,
- ggf. Vermerk über Zeitpunkt und Ergebnis der Einsichtnahme in die Personalakte,
- ggf. Hinweise auf sicherheitserhebliche Erkenntnisse, z. B. durch Vorgesetzte oder Kollegen und Kolleginnen der betroffenen Person,
- Nachweis, dass betroffene Person eine sicherheitsempfindliche Tätigkeit ausübt,
- ggf. Unterlagen über etwaige Aktualisierungs- und Wiederholungsüberprüfungen, einschließlich abgegebene Sicherheitserklärungen und Anträge an die mitwirkende Behörde,
- ggf. Unterrichtungen an die mitwirkende Behörde nach Abschluss der Sicherheitsüberprüfung (Nachberichtspflichten),
- ggf. abgelaufene Konferenzbescheinigungen und FMA-Bescheinigungen,
- 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, Abordnung, Versetzung und Ausscheiden,
- Änderungen des Namens, eines Wohnsitzes und der Staatsangehörigkeit,
- Beginn oder Ende einer Ehe, einer Lebenspartnerschaft oder einer auf Dauer angelegten Gemeinschaft,
- 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.

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

Die Allgemeine Verwaltungsvorschrift zum personellen Geheimschutz und zum vorbeugenden personellen Sabotageschutz – **(SÜG-Ausführungsvorschrift – SÜG-AVV)** – konkretisiert zu § 18 Abs. 1 und 2, welche Informationen regelmäßig von der zuständigen Stelle zur Sicherheitsakte zu nehmen sind.

Der oder dem GSB steht hinsichtlich der sicherheitserheblichen Informationen zu einer betroffenen Person ein Beurteilungsspielraum zu (siehe hierzu weitere Hinweise unter Ziff. IV.3).

Es gilt jedoch zu beachten, dass bei Dokumenten oder Informationen, die von der betroffenen Person freiwillig vorgelegt und damit von ihr selbst als verfahrensfördernd angesehen werden, trotzdem zu prüfen ist, ob sie sicherheitserheblich sind. Beim Verakten ist unbedingt darauf zu achten, dass personenbezogene Daten Dritter dauerhaft unkenntlich zu machen sind (siehe hierzu weitere Hinweise unter Ziff. IV.2). Offensichtlich sachfremde Unterlagen dürfen nicht zur Sicherheitsakte genommen werden.

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

§ 15a SÜG konkretisiert für den öffentlichen Bereich **§ 18 Abs. 2 SÜG** dahingehend, welche Informationen zur betroffenen Person die personalverwaltende Stelle an die oder den GSB weitergeben muss. Diese Daten sind auch in der Sicherheitsakte aufzunehmen. Dazu zählen:

- Umsetzung, Abordnung, Versetzung und Ausscheiden aus dem Dienst,
- Änderungen des Familienstandes, des Namens, des Vornamens, des Geschlechtseintrages, eines Wohnsitzes und der Staatsangehörigkeit,
- Anhaltspunkte für Überschuldung, insbesondere Pfändungs- und Überweisungsbeschlüsse, Mitteilungen über abgeschlossene Insolvenzverfahren sowie Beschlüsse zur Eröffnung eines Insolvenzverfahrens und zur Restschuldbefreiung,
- Strafverfahren und Disziplinarsachen sowie dienst- und arbeitsrechtliche Maßnahmen,
- Nebentätigkeiten,
- sonstige Erkenntnisse, die für die sicherheitsmäßige Beurteilung erheblich sein können.

Weitere Hinweise hierzu gibt **die Allgemeine Verwaltungsvorschrift zum personellen Geheimschutz und zum vorbeugenden personellen Sabotageschutz – SÜG-Ausführungsvorschrift (SÜG-AVV) zu § 15a**.

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

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

Es dürfen ausschließlich Informationen übermittelt werden, die der Zweckbindung entsprechen. **§ 21 SÜG** regelt, wann personenbezogene Daten aus der Sicherheitsüberprüfung übermittelt werden dürfen und zu welchen Zwecken. Klassisches Beispiel ist hier die Datenübermittlung an die mitwirkende Behörde nach **§ 21 Abs. 1 Satz 1 Nr. 1 SÜG**. Besondere Vorsicht ist geboten bei der Vorschrift des **§ 21 Abs. 1 Satz 4 SÜG**. Für disziplinar-, dienst- oder arbeitsrechtliche Maßnahmen darf die zuständige Stelle die Daten aus der Sicherheitsüberprüfung nur verarbeiten, wenn dies für den mit der Überprüfung verfolgten Zweck erforderlich ist. Ansonsten ist eine Weitergabe unzulässig. Zulässig wäre eine Übermittlung beispielsweise, wenn sie den Verschlusssachenschutz gewährleistet. Das wäre der Fall, wenn die oder der GSB in einer konkreten Situation personelle Maßnahmen für notwendig erachtet, und eine Person von einer sicherheitsempfindlichen Tätigkeit bzw. Stelle entfernen will (vgl. AVV zu § 21 Abs. 1 Satz 4 SÜG).

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.

Der Anwendungsbereich des § 21 SÜG umfasst jede Datenübermittlung der zuständigen Stelle oder mitwirkenden Behörde. Das SÜG regelt jedoch nicht die Übermittlung von personenbezogenen Daten an verfahrensbeteiligte Stellen von dritter Seite. Hierfür braucht die übermittelnde Stelle eine einschlägige Rechtsgrundlage. Außerdem können weitere Anforderungen – beispielsweise zum Beschäftigten-datenschutz - relevant werden. Am Sicherheitsüberprüfungsverfahren beteiligte Stellen müssen folglich

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

stets prüfen, ob personenbezogene Daten nach dem SÜG erhoben, verarbeitet und übermittelt werden dürfen.

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 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

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

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 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.

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

§ 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 oder dem GHB steht hier in jedem Einzelfall ein Beurteilungsspielraum zu. Aus 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, insbesondere Geburts- und Eheurkunden, Lebensläufe sowie Zeugnisse. Diese sind nur in die Sicherheitsakte aufzunehmen, wenn Sie explizit als Anlage der Sicherheitserklärung gefordert und vom Betroffenen in diesem Zusammenhang beigebracht werden oder wenn sie von der mitwirkenden Behörde nachträglich im Rahmen der Durchführung der Sicherheitsüberprüfung angefordert 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.

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

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 mitwirkende Behörde übermittelt werden. Die Regelungen 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.[6]

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 GSB die einzelnen Schritte der Sicherheitsüberprüfung 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.

[6] 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

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 nach der SÜG-AVV zu § 13 Abs. 6 SÜG, Ziff. 1.1, im Einzelfall eine handschriftliche Ergänzung der Sicherheitserklärung durch den/die GSB möglich. Der Grund der Ergänzung ist jedoch in einem Vermerk zur Akte zu nehmen. Es ist darauf zu 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