Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung bei Datenverarbeitungen in Sicherheitsüberprüfungsverfahren

(Stand 20.10.2021)

I. Was ist Gegenstand dieses Papiers?

Gegenstand dieses Papiers sind die datenschutzrechtlichen Protokollierungsanforderungen für Nutzeraktivitäten in Fachanwendungen, die zum Zwecke der Unterstützung oder Durchführung von Sicherheitsüberprüfungsverfahren nach dem Sicherheitsüberprüfungsgesetz (SÜG) betrieben oder verwendet werden. Das betrifft alle Verarbeitungen zur Verwaltung, Bearbeitung und Dokumentation von Sicherheitsüberprüfungsverfahren einschließlich einer elektronischen Aktenführung. Hierbei können allgemeine Bürosoftware, spezielle Anwendungen für Sicherheits- und Zuverlässigkeitsüberprüfungen oder fachübergreifende Anwendungen zum Einsatz kommen.

Schutzgut des Datenschutzes sind ausschließlich die Rechte und Freiheiten der von der Datenverarbeitung betroffenen Personen. Der Schutz geheimhaltungsbedürftiger Inhalte bei der Verarbeitung von Verschlusssachen im Sinne des § 1 Abs. 2 SÜG bzw. der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) dient hingegen öffentlichen Interessen, insbesondere dem Bestand, lebenswichtigen Interessen und der Sicherheit von Bund und Ländern. Diese Schutzgüter werden im vorliegenden Papier nicht betrachtet. Insoweit gelten die für die entsprechende Schutzbedarfsklasse festgelegten Anforderungen an die IT-Sicherheit. Diese dient der Gewährleistung der Informationssicherheit einer Organisation und schützt die Daten als solche. Die einschlägigen Protokollierungsanforderungen richten sich insoweit nach dem Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI)[1] und dem Umsetzungsplan Bund (UP Bund)[2] in Verbindung mit

[1] Vgl. BMI: Nationaler Plan zur Umsetzung der Informationsinfrastrukturen, Download unter https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/05-12-09/05-12-09-anlage-nr-16.pdf?__blob=publicationFile&v=2.

[2] Vgl. BMI: Umsetzungsplan Bund 2017: Leitlinie für Informationssicherheit in der Bundesverwaltung, Download unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.pdf?__blob=publicationFile&v=3.

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

dem IT-Grundschutz[3] und den IT-Sicherheitsstandards[4] des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Aufgrund der unterschiedlichen Schutzgüter kann es bei den Protokollierungsanforderungen für den Datenschutz und die IT-Sicherheit Überschneidungen geben. Zusammenbetrachtet ergänzen sich die aus den beiden Bereichen resultierenden Protokollierungsanforderungen und sind ggf. kumulativ umzusetzen.

II. Was ist Protokollierung und wozu dient sie?

Werden bei automatisierten Datenverarbeitungen zu allen oder bestimmten Datenverarbeitungsvorgängen systemseitig im Hintergrund bestimmte Transaktionsdaten mitgeschrieben, spricht man von Protokollierung oder Protokolldaten. Hierbei sind mehrere Protokollierungsebenen zu unterscheiden:[5]

- Protokollierung der Nutzeraktivitäten einer Fachanwendung,
- Protokollierung der Systemaktivitäten und Dienste,
- Protokollierung der Administrationstätigkeiten,
- Protokollierung von Schnittstellenaktivitäten.

Die Protokollierung auf Fachanwendungsebene dient aus datenschutzrechtlicher Sicht insbesondere dem Ziel, wirkungsvolle Kontrollmöglichkeiten sowohl für die Datenschutzaufsichtsbehörden als auch für die regelmäßig durchzuführenden Eigenkontrollen der verantwortlichen Stellen zu schaffen. Die Protokolldaten dienen der Überprüfung, ob die verantwortliche Stelle personenbezogene Daten innerhalb der materiell-rechtlich zulässigen Grenzen bzw. Zwecke – u.a. aus dem SÜG – verarbeitet.

Aus den protokollierten Verarbeitungsvorgängen entsteht ein System von Spuren über die Historie (Erhebung, Veränderung, Löschung) und ggf. die Verwendung (Abfrage / lesender Zugriff,

[3] Vgl. BSI: IT-Grundschutzkompendium (GSC), Baustein OPS.1.1.5 Protokollierung, Stand Februar 2021, Download unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html.

[4] Vgl. BSI: Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen, Version 1.0a vom 25.02.2021, Download unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0a.pdf?__blob=publicationFile&v=5.

[5] Vgl. zu den verschiedenen Ebenen Baustein 43 „Protokollieren“ zum Standarddatenschutzmodell der DSK, Version 1.0a, Stand 2. September 2020, Download unter https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Protokollieren_V1.0a.pdf.

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

Offenlegung einschließlich Übermittlung) eines einzelnen Datums innerhalb eines automatisierten Verarbeitungssystems.

Die Fachanwendungsebene einschließlich ihrer (Fach-)Protokollierung muss auf einer sicheren IT-Infrastruktur einschließlich der Protokollierung aller anderen Ebenen aufbauen. Dies ist eine Voraussetzung, um die Integrität der Protokolldaten auf der Fachanwendungsebene zu gewährleisten. So sind auch die Protokolldaten in der Form zu sichern, dass eine Abänderung nicht möglich ist. Ein übergreifendes IT-Sicherheitskonzept sowie Datenschutzkonzept einschließlich Protokollierungskonzept müssen vorhanden sein.

Für die Protokolldaten zur Fachanwendung und für die Protokolldaten auf anderen Ebenen sind mehrere zumindest logisch getrennte Datenbestände zu führen, da die Löschfristen bzw. -pflichten sowie Rechte- und Rollenkonzepte voneinander unabhängig sein können. Aus den Protokolldaten hat sich zudem die Löschung der Daten aus der Fachanwendung zu ergeben.

Dementsprechend handelt es sich bei sogenannten Änderungshistorien oder Versionierungen im Originaldatenbestand nicht um geeignete Protokolldaten, sondern um eine eigenständige technische und organisatorische Maßnahme (TOM), deren Umsetzung unter bestimmten Voraussetzungen angezeigt sein kann. Versionierung bezeichnet hier und im nachfolgenden Text immer eine Versionsverwaltung innerhalb des Originaldatenbestandes. Davon zu unterscheiden und hier nicht gemeint ist das bloße Anlegen einer neuen Datei (z.B. Abspeichern der neuen Version einer Tabelle als eigenständige Datei unter neuem Namen).

Von der Protokollierung zu unterscheiden ist auch die Dokumentation. Diejenigen Tatsachen, die die rechtliche Zulässigkeit von Verarbeitungsvorgängen begründen, sind nicht Teil der Protokollierung, sondern der (fachlichen) Dokumentation. Behörden unterliegen einer Pflicht zur ordnungsgemäßen Aktenführung mit dem Ziel der vollständigen Dokumentation des Verwaltungshandelns. Das schließt alle aus datenschutzrechtlicher Perspektive relevanten Tatsachen (Lebenssachverhalt) und Wertungen (z.B. Ermessensausübung, Prognoseentscheidung) ein, die zu einem der gemäß § 76 Abs. 1 BDSG protokollierungspflichtigen Verarbeitungsvorgänge führen. Die datenschutzrechtlich relevante Dokumentation muss in dem zum betreffenden Verarbeitungsvorgang gehörenden Aktenrückhalt niedergelegt sein. Für nichtöffentliche Stellen ergibt sich eine entsprechende Dokumentationspflicht indirekt daraus, dass sie als verantwortliche Stelle letztlich die Beweislast für die Rechtmäßigkeit der Verarbeitung tragen (Nachweispflicht).

III. Welche Protokollierungsregelungen für Fachanwendungen gelten im SÜG?

Eine spezifische Regelung zur Protokollierung enthält das SÜG ausschließlich für Abrufe aus elektronisch geführten Sicherheitsüberprüfungsakten (bei den mitwirkenden Behörden).

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

§ 18 Abs. 7 SÜG legt folgenden Mindestinhalt für diese Protokolle fest:

- Zeitpunkt, d. h. Datum und Uhrzeit bzw. Zeitstempel,
- Angaben, die die Feststellung der abgefragten Daten ermöglichen, d. h. Identifizierungsmerkmal des betreffenden Datums,
- Angaben zur Feststellung des Abfragenden, d. h. personenbezogene Benutzeridentifikation.

Weitere Protokollierungsanforderungen ergeben sich aus den Anforderungen an die Datensicherheit nach § 36 Abs. 1 Nr. 2 SÜG i.V.m. § 64 BDSG.

IV. Welche Anforderungen ergeben sich aus § 64 BDSG?

Eine Protokollierungspflicht ist in § 64 BDSG nicht ausdrücklich normiert. Vielmehr ist die verantwortliche Stelle nach § 64 Abs. 1 BDSG zur Sicherstellung eines risikoangemessenen Schutzniveaus mittels technischer und organisatorischer Maßnahmen (TOM) verpflichtet.

Die je nach Risiko erforderlichen TOM werden durch Gewährleistungsziele (Abs. 2) und sog. Kontrollmaßnahmen (Abs. 3) näher beschrieben. Zu den Kontrollmaßnahmen gehören u.a. eine Zugriffskontrolle, eine Übertragungskontrolle und eine Eingabekontrolle.

Die Zugriffskontrolle nach § 64 Abs. 3 Nr. 5 BDSG soll gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Die Übertragungskontrolle nach § 64 Abs. 3 Nr. 6 BDSG soll gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Die Eingabekontrolle nach § 64 Abs. 3 Nr. 7 BDSG soll gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind. De facto wird hiermit zumindest für folgende Transaktionen eine Protokollierungspflicht normiert:

- Erhebung / Eingabe von Daten,
- Veränderung von Daten,
- Löschen von Daten.

Ziel der genannten Kontrollmaßnahmen ist die Nachvollziehbarkeit des Werdeganges eines bestimmten Datums von seiner Erhebung bis zur Löschung. Dahinter steht als Grundprinzip oder auch Gewährleistungsziel die Transparenz der Datenverarbeitung.

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

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) beschreibt das Gewährleistungsziel der Transparenz als „die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten wann und für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt. Transparenz ist für die Beobachtung und Steuerung von Daten, Prozessen und Systemen von ihrer Entstehung bis zu ihrer Löschung erforderlich und eine Voraussetzung dafür, dass eine Datenverarbeitung rechtskonform betrieben und in diese, soweit erforderlich, von betroffenen Personen informiert eingewilligt werden kann. Transparenz der gesamten Datenverarbeitung und der beteiligten Instanzen kann dazu beitragen, dass insbesondere betroffene Personen und Kontrollinstanzen Mängel erkennen und ggf. entsprechende Änderungen an der Verarbeitung einfordern können“.[6] Originär entwickelt wurde diese Beschreibung für den DSGVO-Bereich, allerdings kann sie vorliegend zumindest als Anhaltspunkt und Auslegungshilfe herangezogen werden. Die hier beschriebenen Gewährleistungsziele des Datenschutzrechts finden sich im Wesentlichen in allen Bereichen des Datenschutzrechts wieder und zwar unabhängig davon, ob es sich um rein nationale Regelungen oder um Unionsrecht handelt.

Aus den Kontrollmaßnahmen bzw. dem dahinter stehenden Gewährleistungsziel ergeben sich ohnehin keine absoluten Anforderungen an Art und Umfang der erforderlichen TOM. Vielmehr ist im Sinne eines datenschutzrechtlichen Risikomanagements für jede Verarbeitungstätigkeit / Fachanwendung individuell zu bestimmen, wie die TOM für diese Verarbeitungstätigkeit konkret auszugestalten sind, um ein risikoangemessenes Schutzniveau sicherzustellen. Das gilt auch für die jeweiligen Anforderungen an die fachliche Protokollierung. Insbesondere ist hier zu entscheiden, welche Aktivitäten der Nutzerinnen und Nutzer zu protokollieren sind bzw. ob eine vollständige Protokollierung erforderlich ist.

[6] Vgl. DSK: Standard-Datenschutzmodell (SDM), Version 2.0b, verabschiedet auf der 99. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) am 17. April 2020, Download unter https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html. Zum Gewährleistungsziel Transparenz vgl. Ziff. C1.6. Zur Protokollierung als Referenzmaßnahme für Transparenz vgl. Ziff. D1.5. Siehe ergänzend auch Baustein 43 „Protokollieren“ zum Standarddatenschutzmodell der DSK, Version 1.0a, Stand 2. September 2020, Download unter https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Protokollieren_V1.0a.pdf.

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

Um die einschlägigen Risiken besser identifizieren und angemessene TOM entwickeln zu können, kann nach der Methodik einer Datenschutzfolgenabschätzung[7] vorgegangen werden. So kann der Umfang und die Art und Weise der erforderlichen Protokollierung abhängig vom jeweiligen Schutzniveau nachvollziehbar bestimmt werden.

V. In welcher Form und wie lange ist zu protokollieren?

Die betreffenden Informationen bzw. Protokolldaten müssen manipulationssicher sein. Deshalb müssen administrative Zugriffe ausgeschlossen sein oder protokolliert werden.

Aufgrund der engen Zweckbeschränkung von Protokolldaten müssen alle Zugriffe auf Protokolldaten ihrerseits nachvollziehbar sein, d. h. entweder protokolliert oder zumindest im Vier-Augen-Prinzip dokumentiert werden. Als Dokumentation wäre an dieser Stelle beispielsweise ein Vermerk anzusehen, dass anlassbezogen oder stichprobenartig bestimmte (berechtigte) Personen auf Protokolldaten zugegriffen haben.

Für die Speicherdauer von Protokolldaten im Rahmen des § 36 Abs. 1 Nr. 2 SÜG i.V.m. § 64 BDSG gibt es keine ausdrückliche Regelung. Hier kann im Zweifelsfall auf bewährte Standards zurückgegriffen werden, nach denen Protokolldaten am Ende des auf ihre Generierung folgenden Jahres zu löschen sind (vgl. § 18 Abs. 7 SÜG sowie § 76 Abs. 4 BDSG).

VI. Welche Inhalte gehören in die Protokolldaten?

Damit eine Verarbeitung vollständig überprüft werden kann, sind zumindest folgende Angaben in den Protokolldaten erforderlich:

- Identifizierungsmerkmal des betreffenden Datums,
- Art der Transaktion (zutreffende Bezeichnung der Tätigkeit oder des Ereignisses; „Was?“),
- Zeitkomponente (Datum und Uhrzeit bzw. Zeitstempel; „Wann?“),
- Urheber / auslösende Instanz (personenbezogene Benutzeridentifikation; „Wer?“),
- Speicherinstanz (Quelle und Ziel), die die Protokolldaten speichert („Protokollierung durch wen?“).

Auf eine Speicherung von Inhaltsdaten im Protokolldatenbestand sollte nach dem Grundsatz der Datenminimierung im Regelfall verzichtet werden.[8] Je nach Eingriffsintensität können sich aber zusätzliche Anforderungen an die Protokollierung ergeben. Dies kann bei einzelnen Anwendungen im Ausnahmefall bis zum Erfordernis einer Inhaltsvollprotokollierung reichen. Hierbei ist allerdings auch zu berücksichtigen, inwieweit im Originaldatenbestand eine Versionierung implementiert ist

[7] Zur Methodik einer DSFA siehe z.B. Arbeitshilfen des BfDI zur Datenschutzfolgenabschätzung nach § 67 BDSG im Bereich Polizei und Justiz, Ziff. IV.1.b, Download unter https://www.bfdi.bund.de/DE/Fachthemen/Themen-Positionen/Straf-Sicherheitsrecht/Muster_Arbeitshilfen_Downloads.html.

[8] Vgl. DSK: SDM-Baustein 43, S. 4.

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

und ob die Protokolldaten auf eindeutige Weise einer spezifischen Version zugeordnet werden können. Ggf. sind hierfür weitere Maßnahmen erforderlich, die es ermöglichen, Versionierung und Protokolldaten eindeutig miteinander zu verknüpfen (z.B. Benennung oder Nummerierung der Datenfelder).

Die verantwortliche Stelle ist in der Pflicht, die Protokollierung bei jeder spezifischen Anwendung so zu gestalten, dass sie aus Sicht eines verständigen Dritten den Weg und die Entwicklung des Datums mit allen Stationen von der Erhebung bis zur Löschung nachvollziehbar und mit Blick auf Grundrechtseingriffe kontrollierbar macht.[9]

Eine zusätzliche Anforderung für den Bereich des SÜG ergibt sich aus der engen Zweckbindung und den diesbezüglichen Übermittlungsschranken des § 21 SÜG. Um hier eine angemessene Kontrolle sicherzustellen, ist bei solchen Transaktionen zusätzlich immer der Empfänger von Übermittlungen („An Wen?“) in den Protokolldaten zu erfassen.

VII. Welche Ereignisse sind zu protokollieren?

Für folgende Ereignisse ist zu entscheiden, ob diese zu protokollieren sind:[10]

- Abfrage / Lesen von Daten,
- Erhebung / Eingabe von Daten,
- Veränderung von Daten,
- Sperren von Daten,
- Löschen von Daten,
- Kombination von Daten,
- Offenlegung / Übermittlung,
- Nutzung eines automatisierten Abrufverfahrens,
- Aufruf von Programmen.

Welche dieser Ereignisse beim konkreten Einsatz unterschiedlicher Fachanwendungen zu protokollieren sind, ist abhängig von den Verarbeitungsmöglichkeiten, den damit verbundenen Risikoquellen[11] (Fehleranfälligkeit, Missbrauchsmöglichkeiten u.a.) sowie von der Ausgestaltung anderer TOM (insbesondere Zugriffsbeschränkungen). Insoweit können an dieser Stelle keine

[9] Vgl. BfDI: Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung nach § 76 BDSG, Ziff. VI, Download unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Muster_Hinweise_Protokollierung.pdf?__blob=publicationFile&v=2.

[10] Vgl. hierzu DSK: SDM-Baustein 43, S. 4; BfDI: Hinweise zur Protokollierung nach § 76 BDSG, Ziff. VII.

[11] Zu typischen Risikoquellen siehe z.B. DSK, Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, verabschiedet auf der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) am 27. April 2018, Download unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/95DSK_Kurzpapier_18_Risiko.html?cms_templateQueryString=DSK+Kurzpapier+Nr.+18&cms_sortOrder=score+desc.

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

absoluten Anforderungen entwickelt werden. Dies gilt insbesondere mit Blick auf zukünftige Entwicklungen, die noch nicht vorhersehbar sind.

Sind die o.g. Transaktionen mit der betreffenden Anwendung durchführbar, ist im Regelfall davon auszugehen, dass auch eine Protokollierung erforderlich ist, es sei denn, alle Risikoquellen der jeweiligen Transaktion sind durch andere TOM ausreichend abgesichert bzw. es ist auf anderem Wege ausreichende Transparenz sichergestellt.

Der Verzicht auf eine Protokollierung stellt dementsprechend den absoluten Ausnahmefall dar und muss stets durch andere TOM kompensiert werden. Am ehesten kommt dies noch im nichtöffentlichen Bereich bei der (manuellen) Vorgangsverwaltung mittels Tabellenanwendungen oder selbstkonfigurierten Datenbanken in Betracht. Hier wäre dann beispielsweise zur Nachvollziehbarkeit der Transaktionen Eingabe, Veränderung und Löschung mindestens eine dateiinterne Versionierung / Änderungshistorie in Verbindung mit einem Passwortschutz für den schreibenden und lesenden Zugriff auf die Tabelle / Datenbank sowie ergänzender manueller Dokumentation (Wer kannte wann das Passwort?) erforderlich. Im Bereich der Vorgangsbearbeitung ist eine angemessene Protokollierung hingegen nie verzichtbar.

VIII. Anwendungsbeispiele

Nachfolgend sollen einige Anwendungsbeispiele vorgestellt werden, die in der bisherigen Kontrollpraxis des BfDI angetroffen wurden oder sich für die Zukunft abzeichnen. Diese können bei ähnlich ausgestalteten Verarbeitungen als Orientierungshilfe dienen.

Beispiel 1:
Manuelle Vorgangsverwaltung
in selbstkonfigurierten Tabellen / Datenbanken (Bürosoftware)
bei zuständigen oder nichtöffentlichen Stellen

1. Beschreibung:

In einer Tabelle / Datenbank werden (ausschließlich) Textinformationen gespeichert. Mögliche Grundkomponenten sind eine Tabelle für das Sammeln von Daten, Such-, Sortier- und Filterfunktionen, ggf. Formulare zum Eingeben von Daten, eine Suchmaske / Abfragefunktion (ggf. nach kombinierten Kriterien) sowie ggf. eine Berichtfunktion für Auswerteberichte / visuelle Darstellung. Die Datenfelder sind frei konfigurierbar. Ein manueller Import von Daten aus anderen Quellen ist möglich, desgleichen ein manueller Export von Daten. Eine Serienbrieffunktion kann ggf. genutzt werden z. B. zum Generieren von SiBe-Bescheinigungen.

In der konkreten Ausgestaltung enthält die Tabelle / Datenbank ausschließlich Daten von zu überprüfenden und sicherheitsüberprüften Mitarbeitenden ab dem Zeitpunkt ihrer Zustimmung zur Sicherheitsüberprüfung. Die Datenfelder sind beschränkt auf die nach § 20 Abs. 1 SÜG zulässigen Daten: Grunddaten nach § 13 Abs. 1 Nr. 1-6 SÜG, eigene Aktenfundstelle und die der

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

mitwirkenden Behörde, Beschäftigungsstelle, beteiligte Behörden, Daten zur Vorgangsbearbeitung (Wiedervorlage, Löschfrist).

Zweck der Verarbeitung ist die manuelle Vorgangsverwaltung (z. B. Wiedervorlage, Fristüberwachung, Aussonderung, Vorgangssteuerung, Auffinden von Vorgängen). Unter Vorgangsverwaltung ist die rein formale Begleitung eines Vorgangs zu verstehen. Sie dient dem Nachweis des Eingangs, der Bearbeitung und des Verbleibs von Vorgängen.[12]

Die Tabelle / Datenbank wird nicht zu anderen Zwecken genutzt. (Hinweis: Bei solchen Verarbeitungen ist eine Nutzung der gleichen Tabelle / Datenbank zu anderen Zwecken nach Auffassung des BfDI ausnahmslos unzulässig und stellt immer einen Datenschutzverstoß dar.)

Der Zugriff auf die betreffenden Tabellen oder Datenbanken ist durch geeignete TOM auf die/den Geheimschutzbeauftragte/n bzw. SiBe/SaBe sowie deren Stellvertretende und Mitarbeitende beschränkt.

Änderungen der Nutzer und Zugriffsrechte sind durch geeignete TOM nachvollziehbar.

2. Anforderungen an die fachliche Protokollierung:

Folgende Aktivitäten sind zu protokollieren:

- Abfrage / Lesen von Daten,
- Erhebung / Eingabe,
- Veränderung,
- Löschung.

3. Kompensation durch andere TOM

Ist eine Protokollierung der Transaktionen Eingabe, Veränderung und Löschung (Eingabekontrolle) nicht möglich, ist zur Kompensation mindestens eine Versionierung des Originaldatenbestandes[13] sowie ein angemessener Passwortschutz[14] für schreibenden / lesenden Zugriff mit ergänzender manueller Dokumentation (Wer kannte wann das Passwort?) erforderlich.

---

[12] vgl. BT-Drs. 13/1550, S. 37.

[13] z. B. in MS EXCEL existiert eine Änderungsverfolgung bei freigegebenen EXCEL-Arbeitsblättern vgl. Arbeitsblättern vgl. https://support.office.com/de-de/article/Nachverfolgen-von-%C3%84nderungen-in-einer-freigegebenen-Arbeitsmappe-951bdf89-9ee6-4777-b31e-33ad0f594d18, die über die Oberfläche eingerichtet werden kann.

[14] vgl. Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu Passwörtern: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Umgang-mit-Passwoertern/umgang-mit-passwoertern_node.html.

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

Ist eine Protokollierung der Transaktion Abfrage / Lesen von Daten nicht möglich, ist durch andere TOM eine vollständige Nachvollziehbarkeit und personengenaue Zuordnung entsprechender Aktivitäten sicherzustellen (z.B. Zugriff nur im Vier-Augen-Prinzip und mit Dokumentation der Zugriffe, über Anwesenheitsprotokolle oder andere Login-Daten).

Beispiel 2:
Vorgangsbearbeitung und / oder elektronische Aktenführung
in einer Fachanwendung für Sicherheits- und Zuverlässigkeitsüberprüfungen
durch eine zuständige oder nichtöffentliche Stelle

1. Beschreibung:

Daten werden in einer Tabelle / Datenbank gespeichert. Hieraus können unterschiedliche Verzeichnisse und Statistiken generiert werden. Die Datenfelder sind vorkonfiguriert für verschiedene Überprüfungsverfahren auch außerhalb des SÜG (z.B. nach Luftsicherheitsgesetz), darunter Datenfelder für die Informationen nach § 20 Abs. 1 SÜG. Es gibt Freitext-/ Bemerkungsfelder für die Eingabe zusätzlicher Daten. Elektronische Dokumente können als Dateianhänge zu Datenfeldern / Objekten (z.B. Mitarbeiter) gespeichert werden, so dass eine vollständige elektronische Sicherheitsakte nach § 18 Abs. 6 SÜG (öffentliche Stellen) bzw. § 31 SÜG (nichtöffentliche Stellen) geführt werden kann.

Die verantwortliche Stelle verwendet die Datenfelder zu § 20 Abs. 1 SÜG. Ein Datenexport in Listen und Formulare ist möglich, ggf. auch ein Datenaustausch mit Personalmanagementsystemen. Ein Datenaustausch mit dem Geheimschutzserver des BMWi und ein elektronischer Datenaustausch mit anderen Anwendern der gleichen Fachanwendung (z.B. SiBe-Bescheinigungen) sind ebenfalls möglich. Fristen einschließlich Aussonderungsprüffristen werden automatisiert berechnet.

Der Zugriff auf die Fachanwendung und deren Inhalte ist durch ein entsprechendes Rechte- und Rollenkonzept auf die/den Geheimschutzbeauftragte/n bzw. SiBe/SaBe sowie deren Stellvertretende und Mitarbeitende beschränkt z.B. über Nutzerkonten.

Dateianhänge sind – zumindest bei öffentlichen Stellen – nicht durchsuchbar und automatisierte Abgleiche ausgeschlossen (vgl. § 18 Abs. 6 Satz 2 und 3SÜG).

2. Anforderungen an die fachliche Protokollierung:

Wie in Beispiel 1 sind folgende Aktivitäten zu protokollieren:

- Abfrage / Lesen von Daten,
- Erhebung / Eingabe,
- Veränderung,
- Löschung.

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

Eine Kompensation durch andere TOM erscheint hier regelmäßig nicht ausreichend.

Bedingt durch zusätzliche Risiken bei Datenübermittlungen sind außerdem alle Offenlegungen einschließlich Übermittlungen zu protokollieren (Übertragungskontrolle), also konkret mindestens folgende Aktivitäten:

- Datenexport in Listen und Formulare,
- Datenexport an Drucker,[15]
- Datenübermittlungen an Personalverwaltungssysteme,
- Datenübermittlungen im Besucherkontrollverfahren,
- Datenaustausch mit dem Geheimschutzserver des BMWi,
- sonstige Offenlegungen / Übermittlungen.

Soweit automatisierte Abrufe (z. B. aus Personalverwaltungssystemen) möglich sind, sollten entsprechende Aktivitäten zusätzlich protokolliert werden.

Beispiel 3:
Vorgangsbearbeitung und / oder elektronische Aktenführung
in fachübergreifenden Anwendungen
durch eine zuständige oder nichtöffentliche Stelle

1. Beschreibung

Eine fachübergreifende Anwendung stellt für den Bereich SÜG die gleichen Funktionalitäten wie die in Szenario 2 beschriebene SÜG-Fachanwendung bereit. Darüber hinaus wird sie für andere Verfahrensarten zur Vorgangsverwaltung, Vorgangsbearbeitung und ggf. elektronischen Aktenführung genutzt. Dementsprechend enthält sie zusätzliche Funktionalitäten und Datenfelder. Elektronische Dokumente können erstellt und gespeichert werden. Es gibt eine Vielzahl von Nutzern, die verschiedene Verfahrensarten in der Anwendung bearbeiten.

Um die Verwendung unzulässiger Datenkategorien im SÜG-Verfahren auf der einen Seite und die Kenntnisnahme von SÜG-Daten durch Unbefugte auf der anderen Seite zu verhindern, besteht eine logische Trennung der SÜG-Daten von Daten aus anderen Verfahren im Sinne eines „abgeschotteten Bereiches“, der nur mit besonderen Zugriffsrechten gelesen und bearbeitet werden kann.

[15] Einige Anwendungen sehen standardmäßig bereits ein Druckarchiv vor, in dem Zeitpunkt, Nutzer, Drucker und Druckinhalt (als PDF-Datei) vorgehalten werden.

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

2. Anforderungen an die fachliche Protokollierung:

Es sind alle Anforderungen aus den Szenarien 1 und 2 zu erfüllen. Dementsprechend sind mindestens folgende Aktivitäten zu protokollieren:

- Abfrage / Lesen von Daten,
- Erhebung / Eingabe,
- Veränderung,
- Löschung,
- Offenlegung / Übermittlung.

Durch den erweiterten Nutzerkreis besteht hier ein erhöhtes Risiko für Fehler im Rechte- und Rollenmanagement und damit verbundene Verletzungen der Vertraulichkeit. Damit in entsprechenden Fällen eine Kenntnisnahme und Verwendung durch Unbefugte lückenlos nachvollziehbar ist, sind zusätzliche immer folgende Aktivitäten zu protokollieren:

- Abfrage / Lesen von Daten,
- Nutzung eines automatisierten Abrufverfahrens.

Sofern die Anwendung folgende Aktivitäten ermöglicht, sind diese zusätzlich zu protokollieren:

- Kombination von Daten,
- Aufruf von Programmen.

Eine Kompensation durch andere TOM erscheint hier regelmäßig ausgeschlossen.

3. Weitere Besonderheiten

Wenn in fachübergreifenden Anwendungen Daten verarbeitet werden, die unterschiedlichen Datenschutzregimen (z.B. auch DSGVO oder JI-Richtlinie/BDSG) unterfallen, sind für jeden Datentyp die spezifischen Anforderungen sicherzustellen (z.B. Eintrag ins Verfahrensverzeichnis, Datenschutzfolgenabschätzung, Protokollierung nach § 76 BDSG). Somit ist die Anwendung erst dann rechtskonform, wenn die entsprechenden Anforderungen aus den unterschiedlichen Regimen in Gänze umgesetzt worden sind.

Beispiel 4:
Verarbeitung von SÜG-Daten durch mitwirkende Behörden

Was die mitwirkenden Behörden betrifft, so dürfen diese nach § 20 Abs. 2 SÜG bestimmte Daten aus dem Sicherheitsüberprüfungsverfahren zur Erfüllung ihrer Aufgaben verarbeiten und sind hierbei nicht auf die Aufgabenerfüllung nach dem SÜG beschränkt. Dementsprechend gelten hier keine spezifischen Protokollierungsanforderungen für Sicherheitsüberprüfungsverfahren, sondern es greifen die spezifischen Protokollierungsanforderungen an das jeweils eingesetzte Fachverfahren. Allerdings darf dies nicht dazu führen, dass Daten aus dem

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

Sicherheitsüberprüfungsverfahren ab Übermittlung an die mitwirkenden Behörden einem geringen Schutzniveau unterfallen. Deshalb sind hier im Regelfall mindestens die Protokollierungsanforderungen aus Beispiel 3 zu erfüllen.

Soweit nach § 20 Abs. 2 Satz 2 SÜG die mitwirkende Behörde bestimmte Daten (Grunddaten nach § 13 Abs. 1 Nr. 1 bis 6 SÜG der betroffenen Person und der mitbetroffenen Person und die Aktenfundstelle) auch in Verbunddateien speichern darf, dient auch dies nicht ausschließlich der Aufgabenerfüllung nach dem SÜG. Insofern gelten auch hier die spezifischen Protokollierungsanforderungen an die Verbunddatei. Zum Erhalt des Schutzniveaus gilt auch hier das im vorherigen Absatz Gesagte, wonach im Regelfall mindestens die Anforderungen aus Beispiel 3 zu erfüllen sind.

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