Das Verfahrensverzeichnis

Übersicht über die Verfahren automatisierter Verarbeitungen nach § 4g Absatz 2 Bundesdatenschutzgesetz (BDSG)

www.bitkom.org

bitkom

Herausgeber

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Gesa Diekmann | Leiterin Wissenschaftlicher Dienst
T 030 27576-190 | g.diekmann@bitkom.org

Autoren

- Wolfgang Braun, Konzerndatenschutzbeauftragter Giesecke & Devrient GmbH
- Heiko Gossen, Geschäftsführender Gesellschafter migosens GmbH
- Dr. Hartmut Hässig, Datenschutzbeauftragter EMC Deutschland GmbH
- Lars Kripko, Berater Datenschutz und externer Datenschutzbeauftragter T-Systems Multimedia Solutions GmbH
- Ilona Lindemann, Datenschutzbeauftragte gkv informatik GbR
- Christian Wagner, Datenschutzbeauftragter Nokia Solutions and Networks GmbH & Co. KG
- Stephan Weinert, Datenschutzbeauftragter Computacenter AG & Co oHG

Vorwort zur Version 3.0

Mit fortschreitender Digitalisierung der Wirtschaft sind immer mehr Unternehmen gefragt, über die Verarbeitung personenbezogener Daten Transparenz zu schaffen und Auskunft zu erteilen. Damit steigt die Notwendigkeit einer Handreichung, die sowohl dem neubestellten betrieblichen Datenschützer den Einstieg erleichtern, als auch erfahrenen Datenschützern Gewissheit im Umgang mit den gesetzlichen Anforderungen geben soll.

Änderungen in der Gesetzgebungs- und Aufsichtspraxis bis Dezember 2015 wurden berücksichtigt. Im Dezember 2015 wurde das Trilogverfahren zur EU-Datenschutzgrundverordnung (EU-DS-GVO-E) abgeschlossen. Sie wird nach Ende der Übergangsfristen Mitte des Jahres 2018 weite Teile des geltenden Datenschutzrechts ablösen. Auch die Vorgaben zur Führung eines Verfahrensverzeichnisses werden sich 2018 ändern, da zwar die allgemeine Meldepflicht nach § 4d Abs. 1 BDSG entfällt, gleichwohl eine allgemeine Dokumentationspflicht für die verantwortliche Stelle und auch Auftragsdatenverarbeiter bestehen bleibt (Artikel 28 DS-GVO-E). Da diese wiederum Informationen zur verantwortlichen Stelle, dem Zweck der Verarbeitung, Daten- und Personenkategorien, Übermittlungen sowie Löschfristen und Sicherungsmaßnahmen umfasst, wird weiterhin das Datenschutzmanagement dokumentiert werden müssen, sofern der Betrieb nicht gemäß §28 Abs.4 EU-DS-GVO-E befreit ist. Außerdem wird zukünftig bei zahlreichen Anwendungen Art. 33 EU-DS-GVO-E ein »privacy impact assessment« erforderlich, also eine risikobasierte Folgenabschätzung. Auch hierfür ist eine genaue Dokumentation empfehlenswert. Die vorliegende Publikation deckt also nicht nur den Zeitraum bis 2018 ab, sondern kann Basis der Anpassung an die dann anzuwendenden Vorschriften sein.

Besonderer Dank gilt den Autoren des vorliegenden Leitfadens, deren Expertise und Engagement das Entstehen dieses Leitfadens ermöglicht hat:

- Wolfgang Braun, Konzerndatenschutzbeauftragter Giesecke & Devrient GmbH
- Heiko Gossen, Geschäftsführender Gesellschafter migosens GmbH
- Dr. Hartmut Hässig, Datenschutzbeauftragter EMC Deutschland GmbH
- Lars Kripko, Berater Datenschutz und externer Datenschutzbeauftragter T-Systems Multimedia Solutions GmbH
- Ilona Lindemann, Datenschutzbeauftragte gkv informatik GbR
- Christian Wagner, Datenschutzbeauftragter Nokia Solutions and Networks GmbH & Co. KG
- Stephan Weinert, Datenschutzbeauftragter Computacenter AG & Co oHG

Berlin, den 22.03.2016

Inhalt

1 Einführung

Datenschutz nimmt eine wichtige Rolle in der modernen Datenverarbeitung ein und gewinnt auch an wirtschaftlicher Bedeutung. Dies zeigt sich nicht nur durch mehr mediale Aufmerksamkeit auf sensible Gesetzesvorhaben und Datenschutzverstöße, sondern auch in der vermehrten Wahrnehmung der Betroffenenrechte. Wesentliche Merkmale des europäischen Datenschutzrechts sind neben dem Verbotsprinzip mit Erlaubnisvorbehalt vor allem die Auskunftsrechte und Transparenzanforderungen gegenüber den Betroffenen.

Ohne eine entsprechend aussagekräftige und aktuelle Dokumentation ist sowohl die Gewährleistung der Betroffenenrechte, als auch der Nachweis datenschutzrechtlicher Pflichterfüllung gegenüber den Aufsichtsbehörden aufwändig und vor allem unsicher.

Das Verfahrensverzeichnis ist eine Dokumentationsform und zentrales Instrument des Datenschutzrechts zur Umsetzung dieser Transparenzpflichten. Auf Antrag kann grundsätzlich jedermann Einsicht erhalten. Damit können auch Kunden, Mitarbeiter und andere Partner in spe bereits vor einer wirtschaftlichen Beziehung die Auswirkungen der Datenverarbeitung abschätzen.

Der folgende Leitfaden erklärt Begriffe und Grundlagen des Verfahrensverzeichnisses und erläutert den Prozess zur Erstellung einer solchen Dokumentation. Die Autoren dieses Leitfadens, Datenschutzbeauftragte von Unternehmen, legen besonderes Augenmerk auf die praktische Umsetzbarkeit; unabhängig von der Unternehmensgröße.

2 Das Verfahrensverzeichnis

2.1 Begriffsbestimmungen

Das Bundesdatenschutzgesetz schreibt in den §§ 4d, 4e und 4g die Inhalte eines Verzeichnisses der vorgenommenen Datenverarbeitungen vor, weil für Verfahren der automatisierten Verarbeitung von personenbezogenen Daten grundsätzlich eine ↗Meldepflicht besteht.

Die Inhalte dieser Dokumentation sind zum Teil für jedermann auf Anfrage verfügbar zu machen. Andere Inhalte, wie die konkreten technischen und organisatorischen Maßnahmen, sind nur zur internen Verwendung zu dokumentieren und nur bei Prüfung durch die Datenschutzaufsichtsbehörden vorzulegen. Dadurch hat der Gesetzgeber die Interessen an Transparenz auf der einen Seite mit den Interessen an der Wahrung von Betriebs- und Geschäftsgeheimnissen auf der anderen Seite ausgeglichen.

Der Datenschutzbeauftragte steht in der Praxis vor der Frage, welche Form diesen unterschiedlichen Zielrichtungen des Verfahrensverzeichnisses genügt. Bewährt haben sich die folgenden beiden Lösungsansätze: Zum einen kann eine Dokumentation erstellt werden, aus der im Falle eines Antrags auf Einsichtnahme durch »jedermann« die nichtöffentlichen Inhalte entfernt werden. Zum anderen können zwei unterschiedliche Dokumentationen erstellt werden, wobei das öffentlich zugänglich zu machende Verfahrensverzeichnis immer eine Teilmenge des internen Verfahrensverzeichnisses ist.

Merke

In der Praxis werden oft unterschiedliche Begriffe für diese gesetzlich geforderte Dokumentation verwendet In diesem Leitfaden wird die zur öffentlichen Kenntnisnahme gedachte Dokumentation **öffentliches Verfahrensverzeichnis** genannt, in Praxis und Literatur auch als »Jedermannverzeichnis« oder Verfahrensregister beschrieben. Die gesonderte und nur zur internen Verwendung genutzte Dokumentation, welche alle Informationen enthält, wird in diesem Leitfaden als **internes Verfahrensverzeichnis** bezeichnet, andernorts – wie auch in früheren Versionen dieses Leitfadens – auch als Verarbeitungsübersicht beschrieben.

2.2 Ziel und Zweck des Verfahrensverzeichnisses

Das Verfahrensverzeichnis dient der Transparenz über die Verarbeitung personenbezogener Daten und der rechtlichen Absicherung des Unternehmens. Es dient dem betrieblichen Datenschutzbeauftragten, sowie der Aufsichtsbehörde zur Erfüllung ihrer Aufgaben. Dabei muss der Datenschutzbeauftragte nach § 4g Abs. 2 BDSG das Verfahrensverzeichnis auf Antrag jedermann verfügbar machen. Außenstehende und Betroffene sollen die Verarbeitung personenbezogener Daten innerhalb der verantwortlichen Stelle abschätzen können. Beispielsweise können Bewerber ein Interesse an der Verarbeitung von Mitarbeiterdaten haben und potentielle Kunden am Verarbeitungszweck und der Speicherdauer personenbezogener Daten interessiert sein.

Das Verfahrensverzeichnis ist somit gleichermaßen Grundlage zur Erfüllung unternehmerischer Pflichten und Hilfsmittel der Tätigkeit eines Datenschutzbeauftragten.

2.3 Der Zusammenhang zwischen Meldepflicht und Verfahrensverzeichnis

Gemäß § 4d Abs. 1 BDSG sind Unternehmen verpflichtet, »automatisierte Verarbeitungen« bei der Aufsichtsbehörde anzumelden, bevor sie diese in Betrieb nehmen. Welche Angaben zur Erfüllung dieser gesetzlichen Meldepflicht zu machen sind, ergibt sich aus § 4e Satz 1 BDSG. Die Aufsichtsbehörde führt diese Angaben in einem für jedermann einsehbaren Register.

Diese gesetzliche Meldepflicht entfällt jedoch in den meisten Fällen, wenn – wie es in der Praxis häufig der Fall ist – das Unternehmen einen betrieblichen Datenschutzbeauftragten bestellt hat. Nur wenn es sich um automatisierte Verarbeitungen handelt, für die geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle zum Zweck der Übermittlung, zum Zweck der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung gespeichert werden, hat dafür eine Meldung an die zuständige Aufsichtsbehörde zu erfolgen.

Die Angaben aus § 4e Satz 1 BDSG muss das Unternehmen gleichwohl immer dokumentieren. Sofern ein Datenschutzbeauftragter bestellt ist, übernimmt das Unternehmen anstelle der Aufsichtsbehörde die Aufgabe, ein Verzeichnis über die meldepflichtigen, automatisierten Verfahren zu führen.

In Unternehmen, die keinen Datenschutzbeauftragten bestellen müssen, ist gemäß § 4g Abs. 2a BDSG der Leiter der verantwortlichen Stelle (also bspw. der Vorstandsvorsitzende oder die Geschäftsführung, bei Einzelunternehmern der Inhaber) verantwortlich für die Erfüllung der Aufgaben nach § 4g Abs. 1 und 2 BDSG. Das heißt, dass die Meldepflicht oder die Verpflichtung zur Erstellung eines Verfahrensverzeichnisses unabhängig von der Verpflichtung zur Bestellung eines Datenschutzbeauftragten zu prüfen ist.

Merke

Ist kein DSB bestellt, betreffen die Vorgaben zur Meldepflicht die Leitung des Unternehmens.

2.4 Verantwortlichkeiten

Bei der Frage, wer das Verfahrensverzeichnis führt, muss zwischen der formalen Verantwortlichkeit einerseits und der praktischen Ausführung im Unternehmen andererseits unterschieden werden. Außerdem ist bei der Definition der Verfahren zu berücksichtigen, ob eine Auftragsdatenverarbeitung oder Funktionsübertragung vorliegt.

2.4.1 Die Geschäftsführung

Die formale Verantwortlichkeit für die Erstellung und ordnungsgemäße Führung des Verfahrensverzeichnisses liegt bei der Unternehmensleitung der verantwortlichen Stelle. Sie hat gemäß § 4g Abs. 2 BDSG dem Datenschutzbeauftragten eine Übersicht über geplante Vorhaben zur Verarbeitung von personenbezogenen Daten mit den erforderlichen Angaben zur Verfügung zu stellen. Zwar übernimmt in der Praxis oftmals der Datenschutzbeauftragte die Führung des Verfahrensverzeichnisses. Insbesondere die Erstellung der einzelnen Verfahrensmeldungen obliegt dabei jedoch der Fachabteilung und nicht dem Datenschutzbeauftragten, der auf die Erstellung hinwirken und Hilfestellung anbieten sollte, aber keine Verantwortung für die Inhalte trägt. Die Verantwortung für die einzelnen Verfahren verbleibt bei den Fachabteilungen und letztlich bei der Leitung der verantwortlichen Stelle.

Mit dem Begriff der verantwortlichen Stelle ist die kleinste juristisch eigenständige Einheit gemeint. Dies ist diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Diese Definition ergibt sich unmittelbar aus Art. 2 der europäischen Datenschutzrichtlinie.[1] Für Unternehmen bedeutet dies, dass die verantwortliche Stelle nicht diejenige Organisationseinheit (Abteilung, Dezernat, Referat, Zweigstelle) eines Unternehmens ist, die die Daten tatsächlich speichert beziehungsweise verarbeitet (zum Beispiel das Rechenzentrum oder die Personalabteilung), sondern immer die juristische Person (zum Beispiel eine GmbH), der diese Organisationseinheit angehört.

Im Datenschutzrecht gibt es also kein sogenanntes Konzernprivileg. Jedes zum Konzern gehörende Unternehmen mit eigenständiger Rechtspersönlichkeit stellt eine eigene verantwortliche Stelle dar. Deshalb muss für jedes Unternehmen innerhalb des Konzerns und alle eigenständigen Tochterfirmen ein eigenes Verfahrensverzeichnis geführt werden.

Merke

Jedes rechtlich eigenständige Unternehmen ist eine eigene verantwortliche Stelle.

2.4.2 Der Datenschutzbeauftragte

Dem betrieblichen Datenschutzbeauftragten kommt gemäß § 4g Abs. 2 S. 2 BDSG die Aufgabe zu, die ihm vom Unternehmen gelieferten Informationen jedermann in geeigneter Weise verfügbar zu machen.

1 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates bildet mittelbar die Grundlage des europäischen Datenschutzrechts und wurde durch das Bundesdatenschutzgesetz (BDSG) und die Landesdatenschutz-gesetzen umgesetzt. Für privatwirtschaftliche Unternehmen maßgebliches Recht ist also das geltende BDSG. Ein Rückgriff auf die Richtlinie dient lediglich der Auslegung von Einzelvorschriften. Zur Jahresmitte 2018 wird die EU-Datenschutzgrundverordnung die Richtlinie und weite Teile des BDSG ablösen.

Führt der Datenschutzbeauftragte das Verfahrensverzeichnis kann er selbst nach Zuarbeit und mit Unterstützung aller Unternehmensbereiche die Erstellung und Aktualisierung steuern, sowie die Qualität der Ergebnisse sichern. Ihm kommt dabei die wichtige Aufgabe zu, den Fachbereichen mit verständlichen Erklärungen und praktischen Beispielen die Erstellung ihrer Meldung über die Verarbeitung personenbezogener Daten zu ermöglichen und das Ausfüllen hierfür verwendeter Vorlagen zu erleichtern. So wirkt er ganz wesentlich auf die Einhaltung des Datenschutzes im Unternehmen hin.

2.4.3 Auftragsdatenverarbeitung und Funktionsübertragung

Wenn ein Unternehmen einzelne Datenverarbeitungsprozesse oder auch seine gesamte Datenverarbeitung auf einen Dienstleister überträgt, wie zum Beispiel im Rahmen von Outsourcing, ist die Frage zu klären, wer die Verzeichnisse führen muss.

Liegt eine Auftragsdatenverarbeitung vor, so verbleibt die datenschutzrechtliche Verantwortlichkeit gemäß § 11 BDSG bei dem Auftraggeber. Das erste abgebende Unternehmen in der Kette – wie sie beispielsweise beim Cloud Computing entsteht – bleibt also die verantwortliche Stelle und ist verpflichtet, das Verfahrensverzeichnis zu führen.

Anders liegt es bei einer Übermittlung, der auch die sogenannte Funktionsübertragung zuzuordnen ist. In diesem Fall liegt die Verantwortlichkeit beim Empfänger und die Pflicht zur Führung des Verfahrensverzeichnisses geht auf den Empfänger über. Abgrenzungskriterien und nähere Erläuterungen finden sich in den begleitenden Hinweisen zur Bitkom-Publikation ↗Mustervertragsanlage zur Auftragsdatenverarbeitung, sowie in den ↗Orientierungshilfen der Aufsichtsbehörden.

2.5 Inhalt und Aufbau des Verfahrensverzeichnisses

Wie beschrieben ist zwischen dem öffentlichen, jedermann zugänglich zu machenden Teil des Verfahrensverzeichnisses und dem internen Verfahrensverzeichnis zu unterscheiden. Das öffentliche Verfahrensverzeichnis ist dabei immer eine Teilmenge des internen Verfahrensverzeichnisses. Der Datenschutzbeauftragte muss sich zu Beginn seiner Tätigkeit entscheiden, wie er das Verfahrensverzeichnis führt. Sein Vorgehen sollte sich am Aufbau und der Komplexität des Unternehmens orientieren. Der Detailgrad des internen Verfahrensverzeichnisses orientiert sich immer an den Anforderungen des Datenschutzbeauftragten und dessen Arbeitsweise. Auf dieser Grundlage kann das, in der Regel weniger detaillierte, öffentliche Verfahrensverzeichnis erstellt werden, das den gesetzlichen Anforderungen an Transparenz gegenüber jedermann genügt. In der Praxis finden sich gleichermaßen Beispiele für das einstufige Vorgehen, bei dem ein Verfahrensverzeichnis angelegt wird, aus dem sich der jedermann zugänglich zu machende Teil herauslösen lässt, sowie für die parallele Arbeit mit öffentlichem und internem Verfahrensverzeichnis in getrennten Dokumenten.

Verfahrensverzeichnis

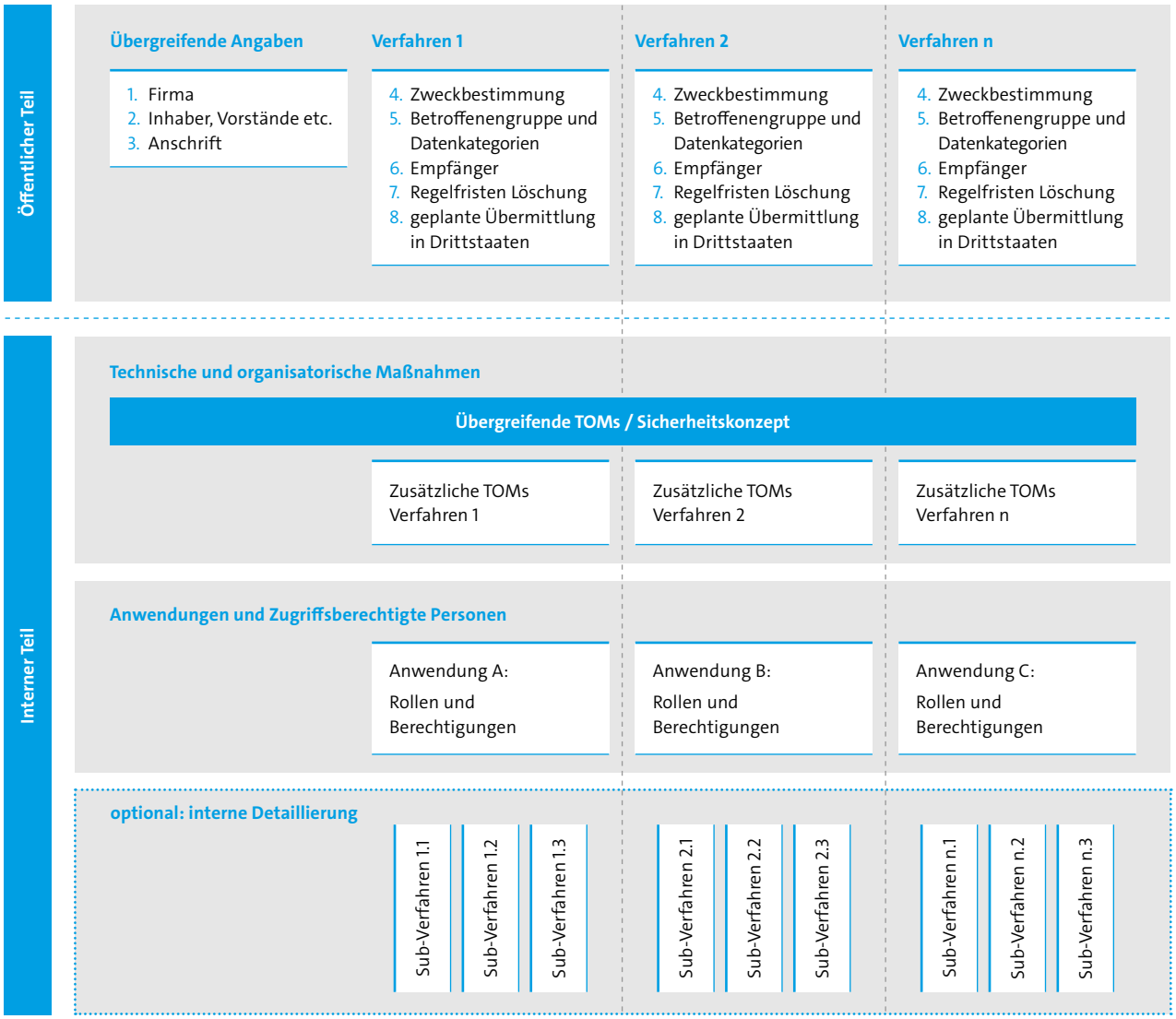


Abbildung 1: Verfahrensverzeichnis

2.5.1 Öffentliches Verfahrensverzeichnis

Gemäß § 4e Abs. 1 Nr. 1 bis 8 BDSG sind im öffentlichen Verfahrensverzeichnis folgende Angaben zu machen:

§ 4e Abs. 1 BDSG	Inhalte	Erläuterung
Nr. 1	Name oder Firma der verantwortlichen Stelle	Diese Angaben dienen im Sinne des Transparenzgebots der zweifelsfreien Identifizierung der verantwortlichen Stelle und der zuständigen Personen.
Nr. 2	Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen	
Nr. 3	Anschrift der verantwortlichen Stelle	
Nr. 4	Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung	Aus der Zweckbestimmung muss sich die Rechtsgrundlage für die Datenverwendung ableiten lassen. In der Praxis werden die Aufgaben und Ziele der einzelnen Prozesse genannt, beispielsweise »Personalmanagement«.
Nr. 5	eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien	Gemeint sind die Personengruppen, die sich aus dem jeweiligen Verfahren ergeben, zum Beispiel »Mitarbeiter« oder »Kunden«.
Nr. 6	Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	Es empfiehlt sich eine Beschreibung der Personengruppen, die Daten planmäßig erhalten sollen. Dies können andere interne und externe Stellen, sowie Dienstleister im Rahmen der Auftragsdatenverarbeitung sein.
Nr. 7	Regelfristen für die Löschung der Daten	In der Regel richtet sich die Löschung nach dem Zweck der Datenerhebung und -nutzung. Zu Löschen ist grundsätzlich unverzüglich nach Fortfall des Zwecks. Ausnahmen ergeben sich insbesondere aus spezialgesetzlichen Aufbewahrungspflichten, zum Beispiel aus dem Steuerrecht oder sonstiger branchenspezifischer Rechtsvorschriften.
Nr. 8	eine geplante Datenübermittlung in Drittstaaten	Zur Beachtung des Transparenzgebots genügt die Nennung der Drittstaaten.

2.5.2 Internes Verfahrensverzeichnis

Wie geschildert bilden die Angaben im öffentlichen Verfahrensverzeichnis eine Teilmenge des internen Verfahrensverzeichnisses. Branchenabhängig und mit Blick auf die jeweiligen Prozesse im Unternehmen müssen im internen Verfahrensverzeichnis detailliertere Beschreibungen ergänzt werden. Die Angaben zu § 4e Abs. 1 Nr. 1 bis 3 BDSG bleiben in der Regel gleich. Der Detailierungsgrad der Beschreibungen zu § 4e Abs. 1 Nr. 4 bis 8 BDSG hängt dagegen von den jeweiligen Unternehmensprozessen ab. Zusätzlich zu den detaillierteren Angaben müssen gemäß § 4e Abs. 1 Nr. 9 BDSG die Sicherheitsmaßnahmen im internen Verfahrensverzeichnisses aufgenommen werden:

§ 4e Abs. 1 BDSG	Inhalte	Erläuterung
Nr. 9	Eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 BDSG und der Anlage zu § 9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.	In der Praxis bewährt sich eine stichpunktartige Aufzählung der getroffenen Schutz- und Sicherheitsmaßnahmen, sowie – soweit vorhanden – der Verweis auf ein detailliertes Datenschutz- und / oder Sicherheitskonzept.

Je nach Organisationsform und Aufbau der IT-Strukturen im Unternehmen kann der Datenschutzbeauftragte vorschlagen, was er zusätzlich zu den Pflichtangaben im internen Verfahrensverzeichnis zur Dokumentation empfiehlt. Für den Datenschutzbeauftragten sind das Verfahrensverzeichnis und die gegebenenfalls in den Fachabteilungen abgefragten ergänzenden Informationen die wichtigsten Hilfsmittel zur Erfüllung seiner Aufgaben.

Es empfiehlt sich, auch die Übersicht der Personen, die Datenzugriff haben, in das interne Verfahrensverzeichnis aufzunehmen. Diese Übersicht ist dem Datenschutzbeauftragten gemäß § 4g Abs. 2 Satz 1 BDSG von der verantwortlichen Stelle zur Verfügung zu stellen.

Im Folgenden werden einige Beispiele für mögliche weitere Ergänzungen aufgezählt, die über die gesetzlichen Mindestanforderungen hinausgehen. Diese Angaben haben sich in der Praxis bewährt, sind aber nicht verpflichtend und auch nicht als abschließende Aufzählung zu verstehen:

- eingesetzte Hard- und Software
- eingesetzte Auftragnehmer im Sinne der Auftragsdatenverarbeitung (sofern nicht aus Empfängern ersichtlich)
- Schnittstellen
- Risikobewertung
- Sicherheitskonzepte
- Rechtsgrundlagen
- Ergebnisse der Vorabkontrolle (hierzu im Folgenden ↗unter Kapitel 3.1)
- verantwortliche Ansprechpartner in den Fachbereichen

In der Anlage finden sich ↗unter 5.1 detaillierte Muster zum Aufbau des öffentlichen und internen Verfahrensverzeichnisses.

2.6 Definition eines Verfahrens

Im BDSG ist der Begriff »Verfahren automatisierter Verarbeitung« nicht näher erläutert. Die Begründung zu Artikel 18 der EU-Datenschutz-Richtlinie spricht von einem Bündel von Verarbeitungen, mit denen eine oder mehrere von der verantwortlichen Stelle definierte Zweckbestimmung(en) durchgeführt werden sollen.

Der Begriff »Verfahren« bezeichnet daher die Gesamtheit an Verarbeitungen, mit deren Hilfe eine Zweckbestimmung oder ein Bündel zusammengehöriger Zweckbestimmungen realisiert wird. Ein Verfahren kann aus einer Vielzahl von DV-Programmen und Dateien bestehen. Wesentlich für die Bestimmung des Verfahrens ist der verfolgte Zweck der Datenverarbeitung.

In der Praxis ist die Frage zu klären, was genau nun ein Verfahren ist sowie welches Verfahren gemeldet und im Verfahrensverzeichnis geführt werden muss.

Einen bewährten Ansatz bietet hierbei die Ausrichtung der Verfahren an:

- Geschäftsprozesse der verantwortlichen Stelle (unsere empfohlene Vorgehensweise)
- Verarbeitungszwecken
- Systeme (Hard- und Software)

2.7 Ausnahmen von der Meldepflicht

Für den Datenschutzbeauftragten ist es wichtig, Kenntnis von allen Verfahren zu haben. Auch Verfahren, in denen die Fachabteilung keine personenbezogenen Daten identifiziert hat, sollten erfasst werden. Bewährt hat sich eine sogenannte »Fehlanzeige« oder »Negativ-Meldung«, für die ein Muster in der Anlage ↗unter 5.3.2 zu finden ist. Anhand dieser Fehlanzeige kann der Datenschutzbeauftragte prüfen, ob tatsächlich keine personenbezogenen Daten verarbeitet werden, zum Beispiel wenn eine Anonymisierung vorgenommen wurde.

Die Frage, welche Verfahren von der Meldepflicht an die Aufsichtsbehörde ausgenommen sind und dementsprechend nicht in das Verfahrensverzeichnis aufgenommen werden müssen, kann den Datenschutzbeauftragten in der Praxis vor Abgrenzungsschwierigkeiten stellen. Es handelt sich um eine Einzelfallentscheidung, die anhand des jeweiligen Verfahrenszwecks getroffen werden sollte und gegebenenfalls mittels der Fehlanzeige dokumentiert wird.

Im Folgenden einige Beispiele für Verfahren, die üblicherweise nicht in die Verfahrensübersicht aufgenommen werden müssen:

- Verfahren, welche keine personenbezogenen Daten, bzw. anonymisierte Daten verarbeiten, wie Produktdatenbanken, Materialdatenbanken, Entwicklungswerkzeuge (z. B. für Hardware, Software oder Mechanik), Maschinensteuerung, ggf. auch z. B. Verfahren der Projekt- oder Fertigungssteuerung.

- Reine Speicherablagen für z. B. Prozess-, Projekt oder Produktunterlagen in welchen auch Bearbeiter und Beteiligte genannt sein können (z. B. Autor und letzter Bearbeiter eines Dokuments, Besprechungsprotokolle, andere Dokumente einschließlich Erstellungs- / Änderungsdatum), soweit diese keine weiteren personenbezogenen Daten enthalten. Diese sind zwar nicht in der Verfahrensübersicht explizit aufzuführen, entsprechend der Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität durch Maßnahmen nach § 9 BDSG zu schützen.

- Nur auf Papier geführte Verfahren, die keine automatisierten Verarbeitungen darstellen, beispielsweise handschriftliche, persönliche Listen.

Diese Beispiele können dem Datenschutzbeauftragten als Orientierung zur Klärung der Meldepflicht dienen, jedoch nicht die Einzelfallentscheidung ersetzen.

2.8 Form des Verfahrensverzeichnisses

Weder in der EU-Richtlinie noch im BDSG gibt es Vorschriften über die Form eines Verfahrensverzeichnisses. In der Praxis ist es meist Aufgabe des Datenschutzbeauftragten, sich seine eigenen Arbeitsunterlagen dafür zu erstellen und die Anforderungen an die verantwortliche Stelle zu formulieren. Hierin liegt auch die Chance, den Ablauf so zu gestalten, wie es für die Erfüllung der Aufgaben der verantwortlichen Stelle hilfreich ist.

Neben der Umsetzung als Formular oder durch Textverarbeitungs-, Tabellenkalkulations-, Datenbanksoftware oder im HTML-Format, kommt auch der Einsatz von spezialisierten Softwareprogrammen in Betracht. Im Anhang ↗unter 5.4 findet sich eine Übersicht einiger Anbieter.

Bei der Auswahl der Form bzw. der technischen Umsetzung wird meist der Datenschutzbeauftragte für das Unternehmen angemessene Anforderungen definieren müssen. Dabei sollten insbesondere

- effektive Zusammenarbeit mit Fachabteilungen,
- Bedienbarkeit (ggf. für Fachabteilungen),
- Verfügbarkeit und Integrität der Verfahrensinformationen

berücksichtigt werden.

2.9 Einsicht oder Veröffentlichung

Die Art und Weise der Information über eine Datenverarbeitung kann vom Datenschutzbeauftragten selbst bestimmt werden. Auch wenn eine mündliche Auskunft rechtlich nicht ausgeschlossen ist, ist sie in der Praxis nicht empfehlenswert, weil sie von den Aufsichtsbehörden als nicht geeignet bewertet werden dürfte. Die Veröffentlichung im Internet ist ebenso praktikabel wie die auf Antrag gezielte Weitergabe der Informationen in Form eines Formulars, z. B. entsprechend des in der Anlage ↗unter 5.1 gezeigten Musters.

Eine Auskunft durch den Datenschutzbeauftragten ist für den Anfragenden kostenfrei. Wünscht der Antragsteller hingegen die Auskunft in einer bestimmten Form, darf der Antragsteller an den Kosten beteiligt werden. Ein generelles Formwahlrecht des Anfragenden gibt es nicht. Weitere Hinweise zu den Anforderungen an die Auskunftserteilung finden sich in einer Publikation des ↗Bayerischen Landesamts für Datenschutz.

3 Erstellen des Verfahrensverzeichnisses

Gemäß § 4g Abs. 2 S. 1 BDSG ist dem Datenschutzbeauftragten von der verantwortlichen Stelle eine Übersicht über die Verfahren automatisierter Verarbeitung personenbezogener Daten zur Verfügung zu stellen.

Die Vorgehensweise des Datenschutzbeauftragten kann typischerweise in mehrere Phasen unterteilt werden.

Grafische Darstellung der einzelnen Phasen als Überblick

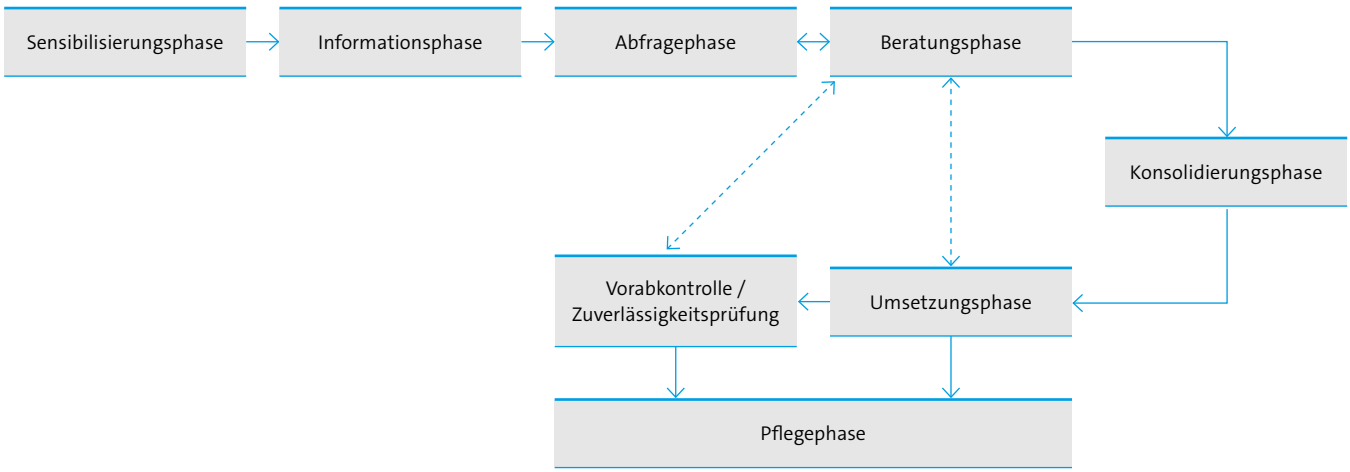


Abbildung 2: Grafische Darstellung der einzelnen Phasen als Überblick

3.1 Sensibilisierungsphase

In einem ersten Schritt sollten die Fachbereiche über die gesetzlichen Vorgaben zur Erstellung eines Verfahrensverzeichnisses und die damit verbundene Zielsetzung in Kenntnis gesetzt werden. Um dem Vorhaben die nötige Bedeutung beizumessen, sollte die Geschäftsführung als verantwortliche Stelle in Verbindung mit dem Datenschutzbeauftragten ein Rundschreiben verfassen und dieses Schreiben gemeinsam mit ihm unterzeichnen. In dem Schreiben sollte der zeitnahe Beginn der Aktion angekündigt, die Bearbeitungszeiten klar vorgegeben und die Bereichsverantwortlichen zur Erfüllung der gemeinsamen Aufgabe aufgefordert werden.

Beispiele für Aktionen des Datenschutzbeauftragten:

- Mailings mit Hinweisen zu Datenschutzmaßnahmen, die jeder Mitarbeiter beachten kann
- Artikel für das Intranet
- Hinweis auf aktuelle Presseartikel zur allgemeinen Sensibilisierung der Mitarbeiter

In der Praxis zeigen sich oftmals ganz grundsätzliche Informationsdefizite, zum Beispiel darüber, dass nur Verfahren zur Verarbeitung personenbezogener Daten in das Verfahrensverzeichnis aufgenommen werden müssen.

3.2 Informationsphase

Die von den Fachbereichen zu benennenden Mitarbeiter, die in die Erstellung des Verfahrensverzeichnisses einbezogen werden, sollten mit dem Vorhaben vertraut gemacht werden, in dem die einzelnen Projektschritte und die zu verwendenden Formulare behandelt werden. Hierbei ist deutlich zu machen, dass der Datenschutzbeauftragte sowohl

- über die bestehenden Anwendungen mit personenbezogenen Daten

als auch

- möglichst frühzeitig über die geplanten neuen Projekte und Anwendungen

in Kenntnis zu setzen ist. Wesentliche Änderungen an bestehenden Anwendungen sind wie neue Anwendungen zu behandeln. Ob es sich hierbei um selbst erstellte oder extern entwickelte Anwendungen handelt, ist gleichgültig.

Beispiele für Aktionen des Datenschutzbeauftragten:

- Erstellung von Übersichten und Erläuterungen, FAQs, Präsentation usw.
- Durchführung von Workshops
- Gemeinsame Bearbeitung eines Musterfalles
- Hinweis auf Fehlanzeige (keine Verarbeitung personenbezogener Daten) mit entsprechendem Musterformular
- frühzeitiger Hinweis auf die Notwendigkeit einer Vorabkontrolle, damit alle Informationen rechtzeitig für die Vorabkontrolle vorliegen (↗hierzu unter 3.7)

3.3 Abfragephase

Wie der betriebliche Datenschutzbeauftragte am effektivsten die notwendigen Informationen abfragt, wird in erster Linie von der Unternehmensgröße abhängen. In größeren Unternehmen können beispielsweise ausführliche Fragebögen erstellt werden. Die vorbereiteten Fragebögen werden zur Erfassung der bestehenden Verarbeitungen mit einem Rückgabetermin an die Fachbereiche versendet.

Als Erstes muss abgefragt werden, ob die Verarbeitung personenbezogene Daten betrifft. Hierbei müssen auch solche Daten berücksichtigt werden, die für sich allein nicht personenbezogen sind, jedoch in Kombination mit anderen Daten einen Personenbezug erhalten können. Ist dies nicht der Fall, kann eine Fehlanzeige nach dem vorgegebenen Muster aufgenommen werden.

Es kann zweckmäßig sein, bereits bekannte (oder typischer Weise in einem Unternehmen zu erwartende) Verfahren schon vorab zu definieren und die Fachbereiche, soweit möglich, eine Zuordnung ihrer Meldung zu diesen Verfahren vornehmen zu lassen. Außerdem wäre zu prüfen, ob es einzelne Verfahren gibt, die zusammengefasst einer gemeinsamen Aufgabe entsprechen, oder ob Aufgaben schon bereits dokumentierten Verfahren zugeordnet werden können. So lässt sich der Detailgrad des Verfahrensverzeichnisses schon von vorneherein festlegen und die Komplexität oft auch reduzieren.

Für kleinere Unternehmen wird häufig auch ein allgemeiner und kurzer Fragebogen über die verwendeten Verfahren ausreichen, an dessen Auswertung sich Gespräche mit den Fachabteilungen zur weiteren Informationserfassung anschließen können.

Beispiele für Aktionen des Datenschutzbeauftragten:

- Verteilung der Fragebögen an die Fachstellen
- Terminverfolgung durch den betrieblichen Datenschutzbeauftragten

3.4 Beratungsphase

Während der Bearbeitungszeit der Meldeformulare durch die Fachbereiche ist trotz der erfolgten Vorinformation erfahrungsgemäß mit zahlreichen Rückfragen zu rechnen. Um die Rückfragen anzunehmen, kann in Abhängigkeit von der Unternehmensgröße, eine vereinfachte Form des Hotline-Dienstes eingerichtet werden. Wo Klärungsbedarf besteht, sollten die strittigen Punkte nach Möglichkeit im direkten Dialog durchgesprochen werden. Ziel sollte dabei sein, einerseits eine Richtigstellung der Meldung zu erreichen und gleichzeitig mit entsprechenden Hinweisen die Qualität künftiger Meldungen zu verbessern.

Beispiele für Aktionen des Datenschutzbeauftragten:

- Einrichtung eines Hotline Dienstes
- Einplanung der nötigen Zeitfenster für Beratung und Durchführung der Maßnahmen
- Klärung offener Fragen bzw. Korrektur offensichtlich unklarer Angaben im Direktkontakt
- Hinweis auf die Notwendigkeit einer Vorabkontrolle (↗hierzu unter 3.7)

3.5 Konsolidierungsphase

Die von den Fachbereichen vorgelegten einzelnen Verfahrensmeldungen sind vom Datenschutzbeauftragten zu strukturieren, d. h. sie müssen auf die einzelnen Aufgabenbereiche verdichtet und inhaltlich konsolidiert werden, um auch für Außenstehende Transparenz zu bieten. Praktisch kann dies bedeuten, dass die einzelnen Verfahrensverzeichnisse des jeweiligen Aufgabenbereichs gesammelt werden und in einer konsolidierten Übersicht für den Bereich zusammengefasst werden. Somit besteht die Möglichkeit, nach unterschiedlichen Detaillierungsgraden Auskünfte zu geben. Durch die gewählte Struktur kann z. B. für die Aufsichtsbehörde gezielt ein Aufgabenbereich dargestellt werden. Im Bedarfsfall kann dann noch auf die einzelnen Anwendungen referenziert werden.

3.6 Umsetzungsphase

Nach Eingang und Strukturierung der Rückmeldungen aus den Fachbereichen müssen diese als Meldung im Verfahrensverzeichnis nachweisfähig dokumentiert werden. Hierzu empfiehlt sich die nachfolgende Vorgehensweise.

Zuerst müssen alle Meldungen auf Vollständigkeit und Richtigkeit geprüft werden. Sind Angaben unvollständig oder nicht korrekt, muss dies mit den jeweiligen Stellen geklärt werden.

Bei Fehlanzeigen ist zu überprüfen, ob anhand der von den Fachbereichen gemachten Angaben bestätigt werden kann, dass keine personenbezogenen Daten betroffen sind. Ggfs. sind hierzu Rückfragen nötig, ansonsten ist die Fehlanzeige als solche zu erfassen.

Bei Meldungen von automatisierten Verarbeitungen ist zu prüfen, ob die vorhandenen Angaben über die technischen und organisatorischen Maßnahmen zum Schutz der Daten ausreichen, um die Wirksamkeit eines angemessenen Schutzniveaus zu bewerten. Kann dies anhand der vorhandenen Informationen nicht bestätigt werden, muss der Datenschutzbeauftragte die Verarbeitung prüfen und die fehlenden Angaben ergänzen (lassen).

Ebenso sollte sich der Datenschutzbeauftragte nicht allein auf die Meldung der Fachabteilung verlassen, sondern die Verarbeitung vor Aufnahme in das Verfahrensverzeichnis selbst überprüfen, vor allem, wenn besonders viele oder besonders sensible Daten verarbeitet werden.

Darüber hinaus muss geprüft werden, ob einzelne Verarbeitungen zulässig sind (Zulässigkeitsprüfung) und der Vorabkontrolle unterliegen. Falls ja, ist ebenfalls erst eine Vorabkontrolle durchzuführen, bevor die Verarbeitung freigeben und im Verfahrensverzeichnis erfasst wird.

Ist sichergestellt, dass alle Informationen vollständig und richtig vorhanden sind, müssen diese als Meldung im Verfahrensverzeichnis erfasst werden. Ob hierzu die Meldungen strukturiert in Papierform abgelegt oder elektronisch erfasst werden, kann von der verantwortlichen Stelle selbst festgelegt werden. Soll hierfür ein Softwareprogramm eingesetzt werden, enthält ↗Kapitel 4 Hinweise darauf, was bei der Auswahl eines geeigneten Programmes beachtet werden sollte.

Nachdem alle Meldungen erfasst und gespeichert sind, empfiehlt es sich die jeweilige Verfahrensmeldung durch den zuständigen Fachbereich auf Richtigkeit prüfen und durch Unterschrift bestätigen zu lassen. In diesem Zusammenhang sollte noch einmal explizit darauf hingewiesen werden, dass Änderungen an dem Verfahren dem Datenschutzbeauftragten zu melden sind.

3.7 Vorabkontrolle und Zulässigkeitsprüfung

Der Begriff der Vorabkontrolle ist im § 4d Abs. 5 BDSG definiert und beschreibt die Pflicht des Unternehmens, bei bestimmten geplanten Datenverarbeitungen die Überprüfung des Verfahrens durch den Datenschutzbeauftragten abzuwarten, bevor mit der Verarbeitung begonnen werden kann. Unabhängig von den Fällen, in denen der Datenschutzbeauftragte zur vorherigen Prüfung gesetzlich verpflichtet ist, ist er immer bei Einführung oder Änderungen an Verfahren rechtzeitig (§ 4g Abs. 1 Nr. 1 BDSG) einzubeziehen. Damit kann der Datenschutzbeauftragte die verantwortliche Stelle und deren Fachbereiche bei der Umsetzung der datenschutzrechtlichen Anforderungen beraten und die Zulässigkeit der Verarbeitung bewerten bzw. bewerten (Zulässigkeitsprüfung), ob eine Vorabkontrolle erforderlich ist. Je nach Ergebnis dieser Prüfung, kann sich eine Abstimmung und Beratung mit den Fachbereichen anschließen bzw. erforderlich sein. Sind Nachbesserungen am Verfahren durch den Fachbereich erforderlich, erfolgt wieder der Rücksprung in die Beratungsphase.

Der gesetzlich vorgeschriebenen Vorabkontrolle, also der zwingenden Prüfung **vor** Beginn der Verarbeitung, unterliegen automatisierte Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Um diese Vorabkontrolle durchführen zu können, benötigt der Datenschutzbeauftragte ein ordnungsgemäß erstelltes Verfahrensverzeichnis. Laut Rechtsprechung kann die Verarbeitung personenbezogener Daten rechtswidrig sein, wenn eine gesetzlich erforderliche Vorabkontrolle nicht durchgeführt werden konnte, weil das Unternehmen kein ordnungsgemäßes Verfahrensverzeichnis führt (vgl. VG Gießen, RDV 2004, S. 257). Die Eingaben sowie das Ergebnis der Vorabkontrolle sollten nachvollziehbar dokumentiert werden und zu dem jeweiligen Verfahren referenziert abgelegt werden. Das Ergebnis kann auch Bestandteil des internen Verfahrensverzeichnisses werden.

Da das Gesetz keine abschließende Aufzählung der Anwendungsfälle liefert, haben die in § 4d Abs. 5 BDSG genannten Beispielcharakter.

Ebenfalls sind Ausnahmen von der Durchführung einer Vorabkontrolle genannt. Aber auch in diesen Fällen ist es in der Praxis als Datenschutzbeauftragter empfehlenswert, die Erforderlichkeit der verwendeten Datenkategorien sowie eine angemessene Umsetzung der datenschutzrechtlichen Grundsätze wie Datenvermeidung und -sparsamkeit bis hin zu den getroffenen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung zu bewerten und zu dokumentieren sowie die Änderungsanforderungen frühzeitig den Verantwortlichen zu kommunizieren.

3.8 Pflegephase

Die Aktualisierung des Verfahrensverzeichnisses setzt eine permanente Kontaktpflege und Sensibilisierung der fachverantwortlichen Stellen durch den Datenschutzbeauftragten voraus, der auf Meldungen zur Veränderungen der Anwendungsstruktur angewiesen ist und bei Änderungen der gesetzlichen Rahmenbedingungen Anpassungen erwirken muss. Dies kann nur gelingen, wenn er in die relevanten IT- bzw. Geschäftsprozesse eingebunden ist. Als flankierende Maßnahme kann es sinnvoll sein, eine interne Revision zu beauftragen, im Rahmen ihrer Routineprüfungen auch die Aktualität der Verfahrensmeldungen zu kontrollieren. Sofern es keinen Prozess zur laufenden Aktualisierung des Verfahrensverzeichnisses gibt, ist eine Aktualisierung in regelmäßigen Abständen zu empfehlen, z. B. einmal jährlich.

Alternativ bietet es sich an, nach einem angemessenen Turnus, die vorliegenden Verfahrensmeldungen zur Prüfung auf Aktualität an die Fachverantwortlichen zurückzugeben. In einem solchen Prüfturnus sollten die Fachverantwortlichen dann neben der Aktualität der bereits abgegebenen Verfahrensmeldungen auch fehlende Verfahrensmeldungen prüfen. Diese Prüfung der Fachverantwortlichen muss mit der Kontrolltätigkeit des Datenschutzbeauftragten verknüpft werden.

Die Fachverantwortlichen sind in jedem Fall permanent zu sensibilisieren, neue Verfahren rechtzeitig an den Datenschutzbeauftragten zu melden. Schließlich kann der Datenschutzbeauftragte die Notwendigkeit einer gesetzlich vorgeschriebenen Vorabkontrolle nur prüfen, wenn ihm Verfahren vor ihrer Inbetriebnahme gemeldet werden.

Aktionen z. B.:

- Überprüfung der Aktualität von Meldungen der Fachstellen durch die Kontrollfunktionen betrieblicher Datenschutzbeauftragter oder interne Revision

- Einholung einer Bestätigung von den Fachbereichen, dass die bestehenden Meldungen aktuell sind; in regelmäßigen Zeiträumen (unternehmensspezifisch ca. alle ein bis drei Jahre)

4 Softwareprogramme zur Führung des Verfahrensverzeichnisses

Je nach Unternehmensgröße und Ausrichtung ergeben sich andere Kriterien zur Auswahl eines geeigneten Programmes für die Unterstützung bei der Erstellung und Pflege des Verfahrensverzeichnisses. Als wichtigstes Kriterium sollte berücksichtigt werden, ob das Programm durch den Datenschutzbeauftragten allein genutzt werden soll, oder ob auch andere Personen das Programm nutzen und bedienen sollen.

Im Folgenden eine Übersicht der grundsätzliche Funktionen, die jedes Programm bieten muss:
- Darstellung der nach § 4e Abs. 1 BDSG geforderten Pflichtangaben
- Eingabe zusätzlicher Informationen, um betriebliche Anforderungen berücksichtigen zu können
- Sicherung aller eingegebenen Daten (Backupkonzept)
- Ausdruck der eingegebenen Daten zur Erstellung von Reports
- Zugriffschutz gegen unberechtigtes Öffnen des Programmes
- Updatefähigkeit des Programmes, um neue Anforderung oder neue Funktionen berücksichtigen zu können
- einstellbare Datenlöschung

Weitere Funktionen, die ein Programm optional bieten sollte:
- Konfigurierbarkeit der Bedienoberfläche zur Anpassung an persönlichen Bedürfnissen
- Möglichkeit zur Erweiterung und Anpassung der Eingabefelder
- Verschlüsselte Datenablage
- Exportmöglichkeiten zu Textverarbeitungsprogrammen (MS Office / PDF)
- Integrierte Onlinehilfe
- Support durch den Softwarehersteller
- Mehrsprachige Bedienoberfläche
- Konfigurierbare Berichte

Soll ein Programm von mehreren Benutzern bedient werden, damit zum Beispiel die jeweiligen Verfahrensverantwortlichen ihre Verfahren selbst anlegen oder pflegen können, sollte das jeweilige Programm noch folgende Anforderungen erfüllen:

- die Bedienoberfläche sollte intuitiv bedienbar sein
- Netzwerkfähigkeit, um allen Anwendern Zugriff über das interne Firmennetz zu geben
- Schnittstelle zu LDAP bzw. zu Active Directory (AD) um eine effiziente Benutzerverwaltung zu ermöglichen
- Benutzer- und Berechtigungskonzept (Mandantenfähigkeit)
- einstellbare automatische Benachrichtigung an den Datenschutzbeauftragten bei Änderungen durch die Benutzer
- Benachrichtigungsfunktion an die Benutzer als Erinnerung / Aufforderung zur Durchführung notwendiger Eingaben / Aktionen
- Kalender mit Wiedervorlage und Benachrichtigung (Erinnerungs- / Alarmfunktion)

Im Anhang ↗unter 5.4 findet sich eine Übersicht einiger Anbieter.

5 Anhang

5.1 Beispiele für öffentliche Verfahrensverzeichnisse

Wie unter 2.1 beschrieben bilden die Angaben des öffentlich zugänglich zu machenden Verfahrensverzeichnisses immer eine Teilmenge des internen Verfahrensverzeichnisses. Hieraus folgt, dass der Datenschutzbeauftragte eine Dokumentation erstellen kann, aus der im Falle eines Antrags auf Einsichtnahme die nichtöffentlichen Inhalte entfernt werden. Ebenso können zwei unterschiedliche Dokumentationen erstellt werden. Im Folgenden zwei Beispiele für ein öffentliches Verfahrensverzeichnis.

5.1.1 Beispiel für ein öffentliches Verfahrensverzeichnis bei einstufigem Vorgehen in Tabellenform

Die folgenden Angaben sind die gesetzlich geforderten Mindestangaben, die öffentlich zugänglich gemacht werden müssen.

Name und Anschrift der verantwortlichen Stelle	Geschäftsleitung	Leiter der Datenverarbeitung der verantwortlichen Stelle
Mustermann Marketing GmbH Eckstr. 5 60437 Frankfurt **Standort Offenbach** Senefelderstr. 160 63069 Offenbach	**Manfred Mann** Geschäftsführer Frankfurt **Hubert Kah** Geschäftsführer Offenbach	**Peter Kraus** Direktor Frankfurt

Nr.	Zweck	Betroffenengruppen	Datenkategorien	Empfänger	Übermittlung Drittstaaten	Löschfrist
01	Bewerbermanagement	Bewerber	Stammdaten, Daten über Kenntnisse und Fähigkeiten wie Zeugnisse, Lebenslauf, Beurteilungen, Kommunikationsdaten	Recruiting, Fachabteilung, FiBu, Mitbestimmungsgremien, Personaldienstleister	nicht geplant	4 Monate nach Abschluss des Bewerbungsverfahrens; mit Einwilligung des Betroffenen: 2 Jahre nach Eingang
02	Personalmanagement	Beschäftigte i.S.d. § 3 Abs. 11 BDSG	a) Stamm- und Vertragsdaten b) Informationen über Kenntnisse und Fähigkeiten wie Zeugnisse, Lebenslauf und Beurteilungen c) Sozialversicherungsdaten, Abrechnungsdaten wie Lohndaten, Steuerklasse, Konfessionszugehörigkeit d) Bankverbindungsdaten e) Fehlzeiten	Personal, Fachabteilung, FiBu, Mitbestimmungsgremien, SV, FA, Bank	nicht geplant	3 Jahre nach Beendigung des Beschäftigungsverhältnisses, nach Ablauf von handels-, steuer- und sozialversicherungsrechtlichen Aufbewahrungspflichten

Nr.	Zweck	Betroffenen-gruppen	Datenkategorien	Empfänger	Übermittlung Drittstaaten	Löschfrist
03	Reisemanage-ment	Beschäftigte	Buchungs- und Abrechnungsdaten, Buchungspräferenzen, Reisezeiten, Buchungs-historie, Legitimations-daten (Kreditkartennr.)	Internes Reise-management, Reisebüro, Dienstleister Reiseservice-portal, Reise-dienstleister (Fluges, Bahn, Hotel), Visa-dienstleister, FiBu	bei Reisen in Drittländer oder Nutzung von Dienst-leistern aus Drittländern	nach Ablauf von handels-, steuer-rechtlichen Aufbe-wahrungspflichten
04	Fuhrpark-management	Leitende Mitarbeiter, Außendienst-mitarbeiter	Stammdaten, Führer-scheindaten, Abrech-nungsdaten, Versiche-rungsdaten, Daten über besondere Vorgänge, Fahrzeug-schäden, Unfall	internes Fuhrpark-management oder externer Dienstleister, Werkstatt und Servicepartner Versicherung	nicht geplant	
05	Marketing und Vertrieb	a) aktive und ehemalige Kunden b) Interessen-ten c) Webseiten-besucher	zu a & b: Kontakt- und Listendaten, Produkt-interessen, Kommuni-kationshistorie, Bonitätsinformationen zu a: Stamm- und Vertragsdaten Kaufhis-torie zu c: Pseudonymisierte Profile gem. § 15 TMG	Marketing, Vertrieb, Externe Dienstleister	Übermittlung pseudonymi-sierter Trackingdaten an US-Dienst-leister	zu a & b: Bei Widerruf durch Betroffen oder nach 2 Jahren nach Beendigung der Kundenbeziehung zu c: nach 6 Monaten durch Aggregation
06	Leistungs-erbringung 1	a) Kunden b) ehemalige Kunden c) Beschäftigte d) Lieferanten	zu a & b: Stammdaten, Bestell- und Abrech-nungsdaten zu c & d: Stammdaten, Leistungsnachweise			nach Ablauf von handels-, steuer-rechtlichen Aufbe-wahrungspflichten
07	Leistungs-erbringung 2	a) Kunden b) ehemalige Kunden c) Beschäftigte d) Lieferanten	zu a & b: Stammdaten, Bestell- und Abrech-nungsdaten zu c & d: Stammdaten, Leistungsnachweise			nach Ablauf von handels-, steuer-rechtlichen Aufbe-wahrungspflichten
08	Rechnungs-legung	a) Kunden b) ehemalige Kunden c) Beschäftigte d) Lieferanten	zu a & b: Stammdaten, Bestell-, Vertrags-, Abrechnungs- und Zahlungsdaten, Bankverbindungsdaten zu c & d: Stammdaten, Leistungsnachweise	FiBu, Vertrieb, Support	nicht geplant	nach Ablauf von handels-, steuer-rechtlichen Aufbe-wahrungspflichten

Nr.	Zweck	Betroffenen-gruppen	Datenkategorien	Empfänger	Übermittlung Drittstaaten	Löschfrist
09	Kundenbe-treuung	aktive und ehemalige Kunden	Stamm-, Vertrags- und Leistungsdaten, Abrechnungsdaten, Korrespondenz, Vorgangsinformatio-nen wie Support-An-fragen, Zahlungsaus-fälle etc.	FiBu, Vertrieb, Support	nicht geplant	nach Ablauf von Ge-währleistungs- und Garantiepflichten
10	Beschaffung	Beschäftigte von Lieferan-ten	betriebliche Kontakt-daten, ggf. Informatio-nen über Kenntnisse und Fähigkeiten	Einkauf, Lager	nicht geplant; je nach Lieferant in Einzelfällen nicht ausge-schlossen	nach Ablauf von handels-, steuer-rechtlichen Aufbe-wahrungspflichten
11	Steuer- und handelsrecht-liche Nach-weiserbrin-gung, Finanzma-nagement	a) Kunden b) Lieferanten c) Beschäftigte d) Interessen-ten	Stammdaten, Leis-tungs- und Abrech-nungsdaten	FiBu, Controlling	nicht geplant	nach Ablauf von handels-, steuer-rechtlichen Aufbe-wahrungspflichten
12	Unterneh-mens-, Objekt- und Informa-tionssicherheit	Beschäftigte, Kunden, Besucher	Stammdaten und Bilder für Firmenaus-weise, Berechtigungen, Accountinformationen, Sicherheitsprotokolle und Authentifizie-rungsdaten (Zutritt, Zugang, Zugriff, Weitergabe), Ergebnis-se von Routinekontrol-len, Besucherlisten, Raumbuchungsinfor-mationen, Videoüber-wachungsbilder, Kennzeichen Privat-Kfz	Sicherheitsbe-auftragter, Empfang, ggfs. Rechtsabteilung		12 Monate nach Ablauf des Erhe-bungsjahres; 3 Jahre nach Beendigung des Beschäftigungsver-hältnisses

5.1.2 Beispiel für ein öffentliches Verfahrensverzeichnis in Textform

Ein Aufbau nach diesem Muster bietet sich an, wenn internes und öffentliches Verfahrensverzeichnis separat voneinander geführt werden.

Öffentliches Verfahrensverzeichnis

Gemäß § 4g BDSG hat der Beauftragte für den Datenschutz auf Antrag jedermann in geeigneter Weise die in § 4e BDSG festgelegten Angaben verfügbar zu machen.

1. Name und Anschrift der verantwortlichen Stelle:

Mustermann Marketing GmbH
Eckstr. 5
60437 Frankfurt

2. Geschäftsführung:

Manfred Mann (Geschäftsführer)

3. Beauftragter Leiter der Datenverarbeitung:

Peter Kraus

4. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Vertrieb, Verkauf sowie Vermittlung von Produkten und Dienstleistungen und aller damit verbundenen Nebengeschäfte.

Nebenzwecke sind begleitende oder unterstützende Funktionen wie im Wesentlichen die Personal-, Vermittler-, Lieferanten- und Dienstleisterverwaltung.

Videoüberwachung erfolgt zur Sammlung von Beweismitteln bei Vandalismus, Einbruch oder sonstigen Straftaten.

Durchführung der Speicherung und Datenverarbeitung von personenbezogenen Daten für eigene Zwecke sowie im Auftrag und Namen der Konzerngesellschaften gemäß den Dienstleistungsvereinbarungen innerhalb des Konzerns.

5. Beschreibung der betroffenen Personengruppe(n) und der diesbezüglichen Daten oder Datenkategorien

Es werden zu folgenden Gruppen zur Erfüllung der unter 4. genannten Zwecke im Wesentlichen die im Folgenden aufgeführten personenbezogenen Daten bzw. Datenkategorien erhoben, verarbeitet und genutzt:

Kunden (Adressdaten, einschl. Telefon-, Fax- und E-Mail-Daten, Auskünfte, Bankverbindungen), Interessenten / Nichtkunden (Adressdaten, Interessengebiete, Angebotsdaten), Bewerber (im Wesentlichen Bewerbungsdaten, Angaben zum beruflichen Werdegang, zur Ausbildung und Qualifikationen, evtl. Vorstrafen), Mitarbeiter, Auszubildende, Praktikanten, Ruheständler, frühere Mitarbeiter und Unterhaltsberechtigte.

Vertrags-, Stamm- und Abrechnungsdaten (Angaben zu Privat- und Geschäftsadresse, Tätigkeitsbereich, Gehaltszahlungen, Name und Alter von Angehörigen soweit für Sozialleistungen relevant, Lohnsteuerdaten, Bankverbindungsdaten, dem Mitarbeiter anvertrauten Vermögensgegenstände); Daten zur Personalverwaltung und -steuerung; Arbeitszeiterfassungsdaten sowie Zugangskontrolldaten; Terminverwaltungsdaten; Daten zur Kommunikation sowie zur Abwicklung und Kontrolle von Transaktionen sowie der technischen Systeme; Notfallkontaktdaten zu vom Mitarbeiter ausgewählten Personen, die im Notfall kontaktiert werden sollen; Handelsvertreter / Vermittler / Makler / Agenturen (Adress-, Geschäfts- und Vertragsdaten; Kontaktinformationen); Lieferanten / Dienstleister (Adressdaten; Kontaktkoordinaten; Bankverbindungen, Vertragsdaten; Terminverwaltungsdaten; Abrechnungs- und Leistungsdaten); Kontaktpersonen zu vorgenannten Gruppen. Sonstige Personengruppe: Videoaufzeichnungen

6. Empfänger der Daten oder Kategorien von Empfängern

Öffentliche Stellen, die Daten aufgrund gesetzlicher Vorschriften erhalten (z. B. Sozialversicherungsträger, Finanzbehörden, Aufsichtsbehörden).

Interne Stellen, die an der Ausführung der jeweiligen Geschäftsprozesse beteiligt sind (im Wesentlichen: Personalverwaltung, Buchhaltung, Rechnungswesen, Einkauf, Marketing, Allgemeine Verwaltung, Vertrieb, Telekommunikation und EDV).

Externe Auftragnehmer (Dienstleistungsunternehmen) entsprechend § 11 BDSG.

Weitere externe Stellen wie z. B. Kreditinstitute (Gehaltszahlungen, Unternehmen soweit der Betroffene seine schriftliche Einwilligung erklärt hat oder eine Übermittlung aus überwiegendem berechtigtem Interesse zulässig ist).

7. Regelfristen für die Löschung der Daten

Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen erlassen. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht, wenn sie nicht mehr zur Ver-

tragserfüllung erforderlich sind. So werden die handelsrechtlichen oder finanzwirksamen Daten eines abgeschlossenen Geschäftsjahrs den rechtlichen Vorschriften entsprechend nach weiteren zehn Jahren gelöscht, soweit keine längeren Aufbewahrungsfristen vorgeschrieben oder aus berechtigten Gründen erforderlich sind. Kürzere Löschungsfristen werden auf besonderen Gebieten genutzt (z. B. im Personalverwaltungsbereich wie z. B.bei abgelehnten Bewerbungen oder Abmahnungen). Sofern Daten hiervon nicht berührt sind, werden sie gelöscht, wenn die unter 5. genannten Zwecke wegfallen.

8. Geplante Datenübermittlung an Drittstaaten (außerhalb EU)

Datenübermittlungen in Drittstaaten ergeben sich nur im Rahmen der Vertragserfüllung, erforderlicher Kommunikation sowie anderer im BDSG ausdrücklich vorgesehener Ausnahmen. Im Übrigen erfolgt keine Übermittlung in Drittstaaten; eine solche ist auch nicht geplant.

Kontakt zum Beauftragten für Datenschutz:

Email: datenschutz@mustermann-marketing.de

5.2 Beispiel für ein internes Verfahrensverzeichnis bei einstufigem Vorgehen

Für das interne Verfahrensverzeichnis müssen, wie ↗unter 2.5.2 beschriebenen, zusätzlich die Maßnahmen nach § 9 BDSG aufgenommen werden.

Nachfolgend ein Beispiel für das Verfahren Bewerbermanagement:

Je nach Einzelfall empfiehlt es sich darüber hinaus zu prüfen, ob zu den einzelnen Spalten detailliertere Informationen bzw. ob weitere Spalten hinzugefügt werden sollen (z. B. Angaben zu eingesetzter Hard- und Software, verantwortlicher Fachbereich, Ansprechpartner für die Verarbeitung innerhalb der verantwortlichen Stelle, ...).

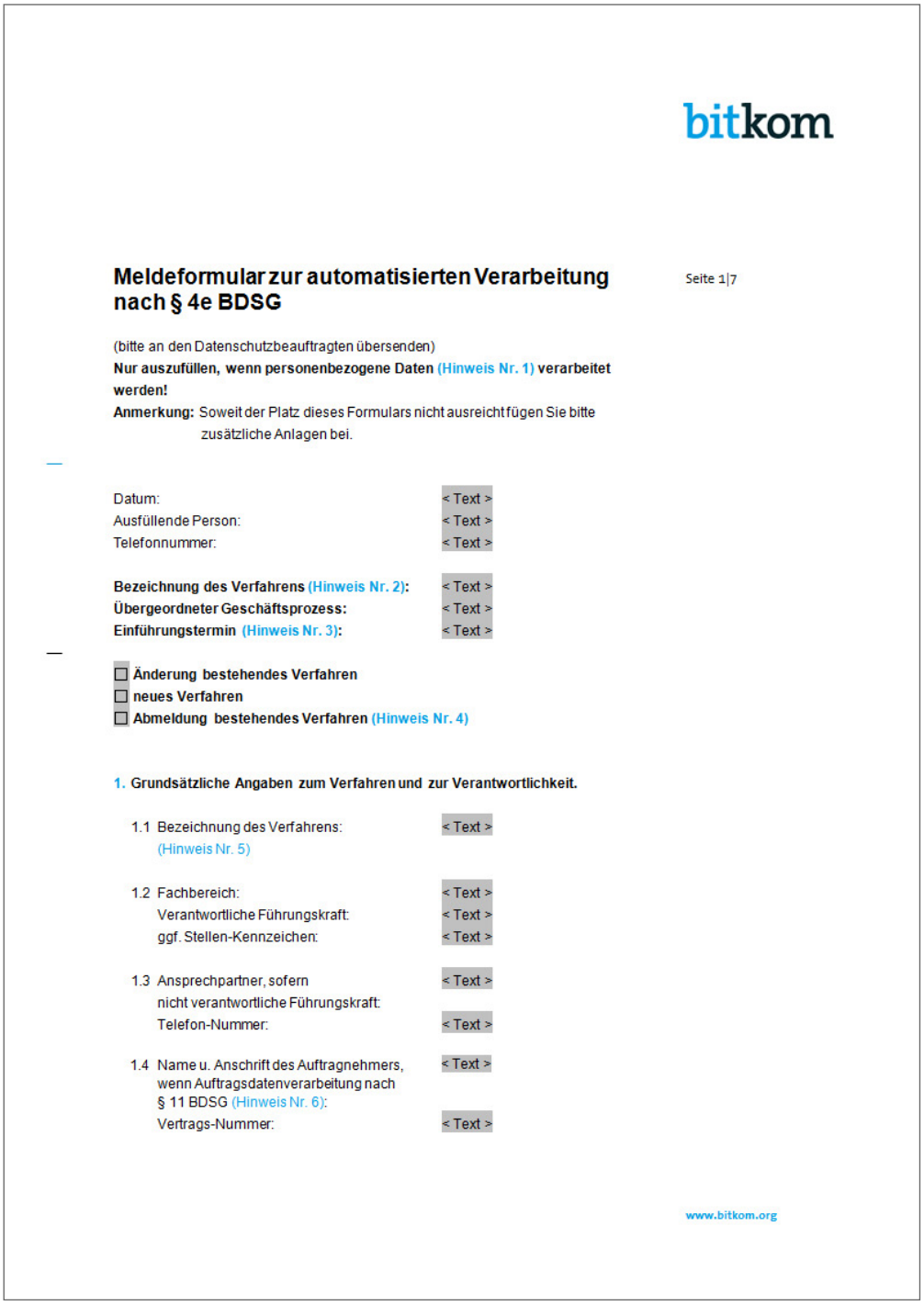
Name und Anschrift der verantwortlichen Stelle	Geschäftsleitung	Leiter der Datenverarbeitung der verantwortlichen Stelle
Mustermann Marketing GmbH Eckstr. 5 60437 Frankfurt **Standort Offenbach** Senefelderstr. 160 63069 Offenbach	**Manfred Mann** Geschäftsführer Frankfurt **Hubert Kah** Geschäftsführer Offenbach	**Peter Kraus** Direktor Frankfurt

Nr.	01
Zweck	Bewerbermanagement
Betroffenengruppen	Bewerber
Datenkategorien	Stammdaten, Daten über Kenntnisse und Fähigkeiten wie Zeugnisse, Lebenslauf, Beurteilungen, Kommunikationsdaten
Empfänger	Recruiting, Fachabteilung, FiBu, Mitbestimmungsgremien, Personaldienstleister
Übermittlung Drittstaaten	nicht geplant
Löschfrist	4 Monate nach Abschluss des Bewerbungsverfahrens; mit Einwilligung des Betroffenen: 2 Jahre nach Eingang
Maßnahmen nach § 9 BDSG	unternehmensspezifische Beschreibung der vorhande-nen Maßnahmen nach § 9 BDSG

5.3 Formulare zur Erfassung der Verfahrensverzeichnisse

Die durchnummerierten Hinweise zu den Formularfeldern finden Sie ↗unter 5.3.5
Die Formulare werden auch als einzelne Word-Dateien ↗zum Download bereitgestellt.

5.3.1 Formular: Meldung einer automatisierten Verarbeitung



bitkom

Meldeformular zur automatisierten Verarbeitung nach § 4e BDSG

Seite 1|7

(bitte an den Datenschutzbeauftragten übersenden)
Nur auszufüllen, wenn personenbezogene Daten (Hinweis Nr. 1) verarbeitet werden!
Anmerkung: Soweit der Platz dieses Formulars nicht ausreicht fügen Sie bitte zusätzliche Anlagen bei.

Datum: < Text >
Ausfüllende Person: < Text >
Telefonnummer: < Text >

Bezeichnung des Verfahrens (Hinweis Nr. 2): < Text >
Übergeordneter Geschäftsprozess: < Text >
Einführungstermin (Hinweis Nr. 3): < Text >

☐ **Änderung bestehendes Verfahren**
☐ **neues Verfahren**
☐ **Abmeldung bestehendes Verfahren (Hinweis Nr. 4)**

1. Grundsätzliche Angaben zum Verfahren und zur Verantwortlichkeit.

1.1 Bezeichnung des Verfahrens: < Text >
(Hinweis Nr. 5)

1.2 Fachbereich: < Text >
Verantwortliche Führungskraft: < Text >
ggf. Stellen-Kennzeichen: < Text >

1.3 Ansprechpartner, sofern nicht verantwortliche Führungskraft: < Text >
Telefon-Nummer: < Text >

1.4 Name u. Anschrift des Auftragnehmers, wenn Auftragsdatenverarbeitung nach § 11 BDSG (Hinweis Nr. 6): < Text >
Vertrags-Nummer: < Text >

www.bitkom.org

bitkom

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung (Hinweis Nr. 7) Seite 2|7

2.1 Zweckbestimmung (Hinweis Nr. 8):
< Text >

2.2 Rechtsgrundlage (zutreffende bitte ankreuzen und erläutern)

☐ Vorrangige Rechtsvorschriften außerhalb des BDSG
(Bitte benennen: Vorschrift, Paragraph, Absatz, Satz)
< Text >

☐ Einwilligung des Betroffenen (§4a BDSG):
Bitte fügen Sie die Einwilligungsklausel hier ein
< Text >

☐ Betriebsvereinbarung:
(Bitte benennen: Genaue Bezeichnung, Paragraph, ggfs. Absatz)
< Text >

☐ Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (§32 BDSG)
< Text >

☐ Vertrag oder Vertragsanbahnung mit dem Betroffenen
(§28 Abs. 1 S. 1 Nr. 1 BDSG)
< Text >

☐ Interessenabwägung (§28 Abs. 1 S. 1 Nr. 2 BDSG):
Bitte benennen Sie die vorrangigen Interessen
< Text >

3. Kreis der betroffenen Personengruppen

Kreis der betroffenen Personengruppen (Hinweis Nr. 9)	Art der Daten / Datenkategorien (Hinweis Nr. 10)	Werden besonderen Arten von Daten verarbeitet? (Hinweis Nr. 11)
		☐ Ja ☐ Nein Welche: < Text >
		☐ Ja ☐ Nein Welche: < Text >
		☐ Ja ☐ Nein Welche: < Text >

bitkom

4. Datenweitergabe und deren Empfänger (Hinweis Nr. 12) Seite 3|7

4.1 Interne Empfänger innerhalb der verantwortlichen Stelle

Interne Stelle (Org-Einheit)	< Text >
Art der Daten	< Text >
Zweck der Daten-Mitteilung	< Text >

4.2 Externe Empfänger und Dritte (jeder andere Empfänger, auch Konzernunternehmen)

Externe Stelle	< Text >
Art der Daten	< Text >
Zweck der Daten-Mitteilung	< Text >

4.3 Geplante Datenübermittlung in Drittstaaten (außerhalb der EU)

Welcher Staat	< Text >
Art der Daten	< Text >
Zweck der Daten-Mitteilung	< Text >

5. Regelfristen für die Löschung der Daten (Hinweis Nr. 13)

Existieren gesetzliche Aufbewahrungsvorschriften oder sonstige einschlägige Löschungsfristen?

☐ Ja, falls ausgewählt bitte benennen: < Text >
☐ Nein

Bitte beschreiben Sie, ob und nach welchen Regeln die Daten gelöscht werden:
< Text >

6. Bereitstellung des Verfahrens
Welche Software oder Systeme werden für die Verarbeitung der Daten innerhalb des Verfahrens eingesetzt?

Bezeichnung	Hersteller	Funktionsbeschreibung	Bereitstellung
< Text >	< Text >	< Text >	☐ Eigenentwickelte / Individual Software ☐ Standard- bzw. Kauf-Software ☐ Cloud-Services
< Text >	< Text >	< Text >	☐ Eigenentwickelte / Individual Software ☐ Standard- bzw. Kauf-Software ☐ Cloud-Services
< Text >	< Text >	< Text >	☐ Eigenentwickelte / Individual Software ☐ Standard- bzw. Kauf-Software ☐ Cloud-Services

bitkom

7. Zugriffsberechtigte Personengruppen (vereinfachtes Berechtigungskonzept) (Hinweis Nr. 14)

Benennung Personengruppen	Berechtigungsrolle	Umfang des Datenzugriffs (Nennung der Datenarten)	Art des Zugriffs	Zweck des Datenzugriffs
< Text >	< Text >	< Text >	☐ Lesen ☐ Schreiben ☐ Löschen	< Text >
< Text >	< Text >	< Text >	☐ Lesen ☐ Schreiben ☐ Löschen	< Text >
< Text >	< Text >	< Text >	☐ Lesen ☐ Schreiben ☐ Löschen	< Text >

Bitte erläutern Sie kurz den Prozess zur Erlangung und Verwaltung der Berechtigungen oder benennen Sie das detaillierte betriebliche Berechtigungskonzept:
< Text > (ggf. als Anlage anfügen)

8. Technische und organisatorische Maßnahmen (§ 9 BDSG) (Hinweis Nr. 15)

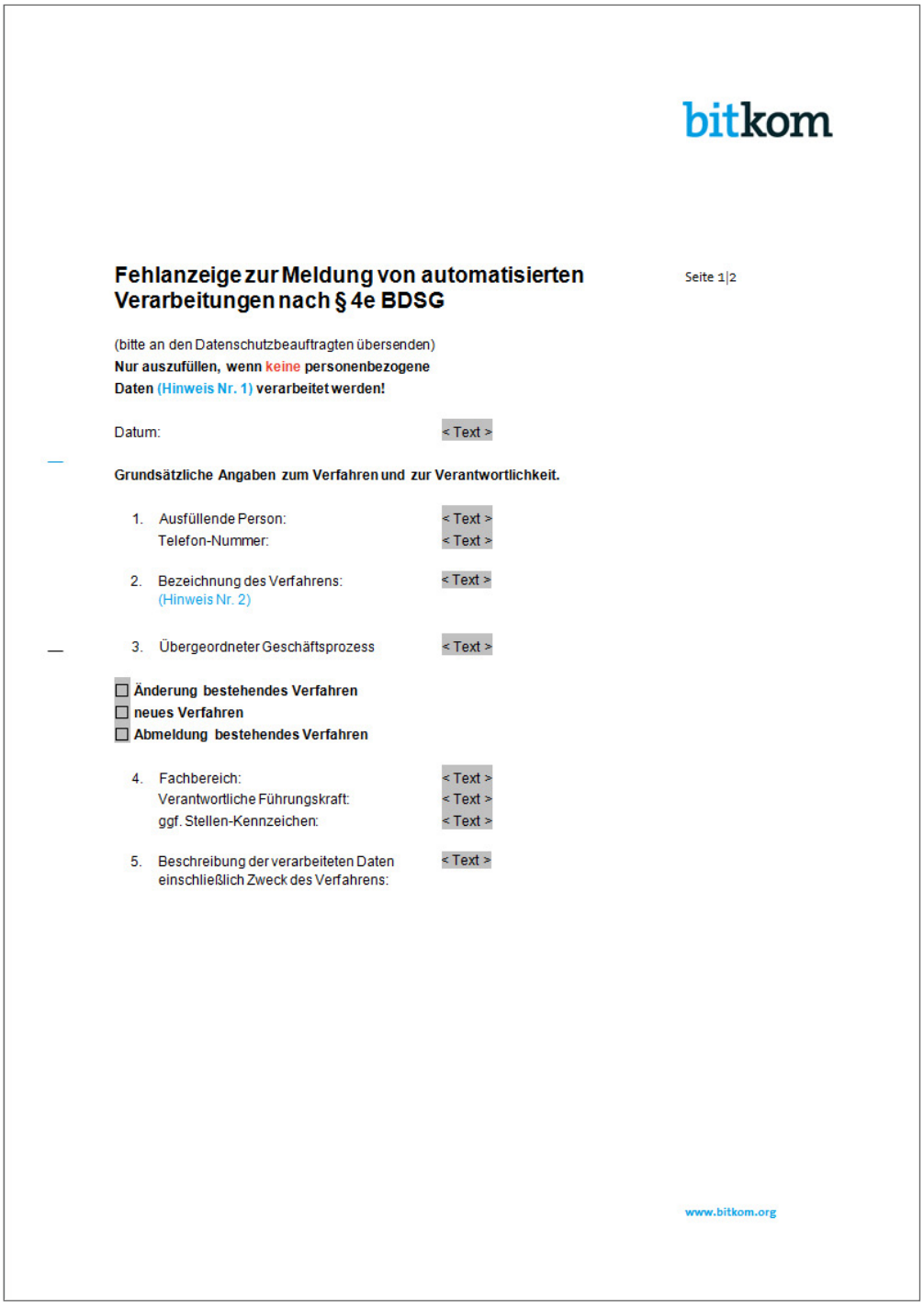
Hinsichtlich der Datensicherheitsmaßnahmen wurde der Bereich IT-Sicherheit eingebunden
☐ Ja
☐ Nein, falls ausgewählt bitte kurze Begründung: < Text >

Die Maßnahmen entsprechen dem allgemeinen Unternehmens-IT-Sicherheitskonzept
☐ Ja
☐ Nein

Bitte Angaben zu den abweichenden, bzw. zusätzlichen Maßnahmen ergänzen:
< Text >

Zutrittskontrolle	< Text >
Zugangskontrolle	< Text >
Zugriffskontrolle	< Text >
Weitergabekontrolle	< Text >
Eingangskontrolle	< Text >
Auftragskontrolle	< Text >
Verfügbarkeitskontrolle	< Text >
Trennungsgebot	< Text >

5.3.2 Formular: Meldung Fehlanzeige



bitkom

Fehlanzeige zur Meldung von automatisierten Verarbeitungen nach § 4e BDSG

Seite 1|2

(bitte an den Datenschutzbeauftragten übersenden)
Nur auszufüllen, wenn keine personenbezogene Daten (Hinweis Nr. 1) verarbeitet werden!

Datum: < Text >

Grundsätzliche Angaben zum Verfahren und zur Verantwortlichkeit.

1. Ausfüllende Person: < Text >
   Telefon-Nummer: < Text >
2. Bezeichnung des Verfahrens: < Text >
   (Hinweis Nr. 2)
3. Übergeordneter Geschäftsprozess < Text >

☐ **Änderung bestehendes Verfahren**
☐ **neues Verfahren**
☐ **Abmeldung bestehendes Verfahren**

4. Fachbereich: < Text >
   Verantwortliche Führungskraft: < Text >
   ggf. Stellen-Kennzeichen: < Text >
5. Beschreibung der verarbeiteten Daten einschließlich Zweck des Verfahrens: < Text >

www.bitkom.org

5.3.3 Formular für interne Prüfvermerke des Datenschutzbeauftragten

bitkom

Formular für interne Prüfvermerke des Datenschutzbeauftragten

Projekt-Nr., bzw. Verfahrensbezeichnung: < Text >

	Datum	Namenszeichen
1. Vorgang geprüft	< Text >	< Text >
2. Meldung im VVZ erforderlich	☐ Ja	☐ Nein
3. Vorabkontrolle erforderlich	☐ Ja	☐ Nein
4. Falls Vorabkontrolle erforderlich:	Ergebnis der Zulässigkeitsprüfung: ☐ Ja ☐ Nein	Anmerkungen: < Text >
5. Wiedervorlage für Verfahrensregister zum Einführungszeitpunkt und Überprüfung der Einführung	< Text >	< Text >
6. Zuordnung und Kontrolle der Auswirkungen auf das interne Verfahrensverzeichnis durchgeführt.; ggf. Anpassung.	< Text >	< Text >
7. Kontrolle der Auswirkungen auf das öffentliche Verfahrensverzeichnis durchgeführt.; ggf. Anpassung.	< Text >	< Text >
8. Ablage beim Datenschutz	< Text >	< Text >

Angestoßene Maßnahmen	Verantwortlicher	Frist
1. < Text >	< Text >	< Text >
2. < Text >	< Text >	< Text >
3. < Text >	< Text >	< Text >

www.bitkom.org

5.3.4 Checkliste zu den technischen und organisatorischen Maßnahmen

Hinweis Nr. 15

Zutrittskontrolle: Wie wird sichergestellt, dass Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen haben, mit denen die personenbezogenen Daten verarbeitet oder genutzt werden?	Sicherheitsbereiche entsprechend dem Schutzbedarf (Besucherbereiche, interne Büros, IT-Räume), Einrichtungen zum Zutrittsschutz (Gebäudesicherung, Wachdienst, Einbruchmeldesystem, Karten- oder schlüsselbasierte Zutrittskontrollsystem), Zutrittsberechtigungen (Personenkreise und Rollenkonzept), Verwaltung der Zutrittsberechtigungen (Verlust der Schließmittel, Ausscheiden und Wechsel in andere Rolle), Protokollierung des Zutritts, Speicherfristen, Ausweistragepflicht, Regelungen zum Zutritt von Dienstleistern und Besuchern.
Zugangskontrolle: Wie ist sichergestellt, dass nur Befugte Zugang zu den Datenverarbeitungssystemen haben?	Authentifizierung (User-ID, Passwort, ggf. Zweifaktor-Authentifizierung), Anforderung an Passworte und deren Kontrolle, Verbot der ungeschützten Aufzeichnung von Passworten, Sperrung des Users nach Fehlversuchen, Vorgehensweise zur erneuten Freischaltung des Users, Rollenkonzept zur Vergabe der Zugangsberechtigungen, Vorgehensweise zur Genehmigung, Vergabe und Rücknahme von Zugangsberechtigungen, routinemäßigen Kontrolle der vergebenen Berechtigungen, Protokollierung des Zugangs und Auswertung von Fehlversuchen, Speicherfristen. Automatische Zugangssperre durch Bildschirmschoner, Anweisung zu Sperrung / Log-off bei Abwesenheit.
Zugriffskontrolle: Wie wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden, Daten zugreifen können und dass die personenbezogenen Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können?	Beschreibung von systemimmanenten Sicherungsmechanismen, evtl. übergeordnetes Zugriffsschutzsystem, Mehraugenprinzip, automatische Prüfung der Zugriffsberechtigung, eingesetzte Verschlüsselungsverfahren, Rollenkonzept zur Vergabe der Zugriffsberechtigungen, Vorgehensweise zur Genehmigung, Vergabe und Rücknahme von Zugriffsberechtigungen, routinemäßigen Kontrolle der vergebenen Berechtigungen, Umsetzung des Rollenkonzepts in den Verfahren, Protokollierung der Zugriffe und Auswertung von Fehlversuchen, Speicherfristen. Bei Online-Zugriffen des Auftraggebers ist hier zu beschreiben, wer beim Auftraggeber für die Ausgabe und Verwaltung von Zugriffsberechtigungen verantwortlich ist.

Weitergabekontrolle: Wie ist sichergestellt, dass Daten bei elektronischer Übertragung während ihres Transportes oder bei Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können? Wie wird überprüft und festgestellt, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist?	Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z. B. Identifizierung und Authentifizierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren und Übertragungstechniken, Regelungen zur Datenträgervernichtung oder zur sicheren Löschung vom Speichermedien, Regelungen zur sicheren Lagerung und zum sicheren Versand von Datenträgern, Regelungen zum Gebrauch von mobilen Datenträgern (CDs, USB-Sticks).
Eingabekontrolle: Wie wird sichergestellt, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind?	Beschreibung der Protokollierung der Systemaktivitäten, Aufbewahrung von Verarbeitungsprotokollen, Verweis auf Eingabeberechtigte (siehe Rollenkonzept), Protokollierung der Eingaben und Speicherfristen.
Auftragskontrolle: Wie wird sichergestellt, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können?	Es sollte hier auf die entsprechenden Weisungen zwischen dem Auftraggeber und Auftragnehmer verwiesen werden, z. B. Weisungsberechtigte beim Auftraggeber und Empfangsberechtigte beim Auftragnehmer, Leistungsbeschreibung und Vorgehensweise bei kurzfristigen Änderungen, Betriebsstörungen, Protokollierung der Auftragsdurchführung durch den Auftragnehmer, Vorgehensweise bei Vertragsende.
Verfügbarkeitskontrolle: Wie wird sichergestellt, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind?	Backup-Konzept (Redundante Systeme, Failover, unterbrechungsfreie Stromversorgung, etc.), Datensicherung (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und sicherem Aufbewahrungsort für Backupmedien), Notfallplan entsprechend möglicher Gefährdungen, Verfahren zum Wiederanlauf, Test der Notfalleinrichtungen.
Trennungsgebot: Wie wird sichergestellt, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können?	Logische Trennung der Daten auf Systemebene, Mandanten-Trennung, Trennung über Zugriffsregelung etc. gemäß Zweckbestimmung des Verfahrens.

5.3.5 Erläuterungen zu den Formularen

Hinweis Nr. 1

»Personenbezogene Daten« sind nach § 3 Nr. 1 BDSG definiert als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, z. B. Name, Geburtsdatum, Anschrift, Einkommen, Beruf, Kfz-Kennzeichen, Konto-oder Versicherungsnummer. Auch pseudonymisierte Daten, zum Beispiel eine IP-Adresse oder Personalnummer, aus denen die betroffene Person indirekt bestimmbar wird, gelten als personenbezogener Daten.

Hinweis Nr. 2

Betriebsinterne Benennung, die Identifikation des einzelnen Verfahrens ermöglicht unter Zuordnung zum jeweiligen Geschäftsprozess in dem die Daten verarbeitet werden.

Hinweis Nr. 3

Geplanter Einführungstermin (Projekte) oder tatsächlicher Einführungstermin.

Hinweis Nr. 4

Nur bei Beendigung der Verarbeitung auszuwählen. Bei Auswahl kann das ursprüngliche Meldungsformular verwendet werden. In Abstimmung mit dem DSB ist über die weitere Verwendung des Datenbestands zu entscheiden, also ob Löschung oder Migration in andere Verfahren erforderlich ist.

Hinweis Nr. 5

Genaue Kennzeichnung des Verfahrens mit Mitteln des allgemeinen Sprachgebrauchs und Hinweisen zur Verarbeitung personenbezogener Daten.

Hinweis Nr. 6

Dient der Sicherstellung einer sorgfältigen Auswahl des Dienstleisters, dem Nachweis eines schriftlichen Vertrags und der Wahrnehmung der Kontrollpflichten.

Hinweis Nr. 7

Zieldefinition der Verarbeitung personenbezogener Daten und Nennung der darauf gerichteten rechtlichen Grundlage (Prinzip des Verarbeitungsverbots mit Erlaubnisvorbehalt).

Hinweis Nr. 8

Konkrete Beschreibung des Zwecks der Datenverarbeitung. Es empfiehlt sich, entsprechende Erläuterungen möglichst unter der im Unternehmen bekannten Terminologie zu formulieren und in Zweifelsfällen Rücksprache mit dem DSB zu halten.

Hinweis Nr. 9

Nennung der durch die Verarbeitung betroffener Personengruppen, z. B. Beschäftigte (Mitarbeiter(-gruppen)), Berater, Kunden, Lieferanten, Patienten, Schuldner, Versicherungsnehmer, Interessenten.

Hinweis Nr. 10
Beispiele für Datenkategorien: Identifikations- und Adressdaten, Vertragsstammdaten, Daten zu Bank- oder Kreditkartenkonten, IT-Nutzungsdaten (z. B. Verbindungsdaten, Logging-Informationen).

Hinweis Nr. 11
Diese »besondere Arten personenbezogener Daten« ergeben sich aus § 3 Abs. 9 BDSG. Hierbei handelt es sich um Daten über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Hinweis Nr. 12
Zweck und Empfänger personenbezogener Daten zur Weiterverarbeitung bzw. Nutzung innerhalb der verantwortlichen Stelle oder im Rahmen einer Übermittlung an Dritte.

»Empfänger« ist jede Person oder Stelle, die Daten erhält, z. B. Vertragspartner, Kunden, Behörden, Versicherungen, ärztliches Personal, Auftragsdatenverarbeiter (z. B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter), oder ein Verfahren, bzw. Geschäftsprozess, an den Daten weitergegeben werden. § 4 e Nr. 8 BDSG fordert die Angabe der geplanten Übermittlungen in Drittstaaten (Nicht-EU-Länder und Nicht-EWR-Länder).

Die Art der Daten oder Datenkategorien ist getrennt nach dem jeweiligen Drittstaat und den jeweiligen Empfängern oder Kategorien von Empfängern anzugeben.

Hinweis Nr. 13
Gemäß § 35 Abs. 2 Nr. 1 BDSG sind personenbezogene Daten zu löschen, wenn der Zweck ihrer Erhebung, Verarbeitung, oder Speicherung weggefallen ist. Unter Beachtung (z.B. steuer-) gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen müssen die Daten nach Zweckfortfall unverzüglich gelöscht werden. Wird keine Löschung ausgewählt oder bei Zweifeln zu Aufbewahrungsfristen und Löschroutinen ist Rücksprache mit dem DSB zu halten.

Hinweis Nr. 14
Skizzierung des Berechtigungsverfahrens und Nennung der berechtigten Gruppen. Sofern vorhanden kann auf ein umfassendes betriebliches Berechtigungskonzept verwiesen werden.

Hinweis Nr. 15
Beschreibung der Schutzmaßnahmen im Hinblick auf die Kontrollziele für die jeweils verarbeiteten personenbezogenen Daten. Im Leitfaden findet sich ↗unter 5.3.4 eine Checkliste mit Kontrollfragen. Im Fall einer festgelegten betrieblichen Sicherheitspolitik im Unternehmen kann der Hinweis auf die Abstimmung mit der Organisationseinheit »IT-Sicherheit« erfolgen.

Ergänzend kann auf die ISO 27001 Bezug genommen werden. Die acht Kontrollziele zur angemessenen Sicherung der Daten vor Missbrauch und Verlust sind dabei nicht abschließend oder als in Gänze verpflichtender Maßnahmenkatalog zu sehen. So könnten aufgrund einer Spezialgesetzgebung zum Datenschutz weitere Kontrollziele und entsprechende Maßnahmen gefordert sein (z. B. aus dem Telekommunikationsgesetz, aus der Sozialgesetzgebung, oder aus den Landesdatenschutzgesetzen).

5.4 Anbieter von Softwareprogrammen zur Erstellung des Verfahrensverzeichnisses

Stand: 29.02.2016

Im Folgenden eine Übersicht zu einigen Anbietern und Produkten, die dem Datenschutzbeauftragten bei der Erstellung des Verfahrensverzeichnisses Hilfestellung geben können. Die Auflistung erhebt keinen Anspruch auf Vollständigkeit und stellt keine Präferenz des Bitkom AK Datenschutz dar. Jeder Datenschutzbeauftragter ist aufgefordert, eigene Qualitätsmaßstäbe an Aufbau und Funktionalität der Produkte anzulegen.

- 2BAdvice: 2B Advice PrIME
  https://www.2b-advice.com/PrIME-DE/PrIME-Home-Datenschutzsoftware
- Black Brain Medien Dienste: DSBBrain2000
  http://www.dsbbrain2000.de/
- Deichmann + Fuchs Verlag: Verfahrensverzeichnis mit den wichtigsten Verfahrensbeschreibungen im Unternehmen
  https://www.deichmann-fuchs.de/datenschutz/verfahrensverzeichnis/verfahrensverzeichnis-mit-den-wichtigsten-verfahrensbeschreibungen-im-unternehmen.artikel.html
- Demal GmbH: DSB Assist
  https://www.demal-gmbh.de/index.php?id=28
- Keck DSB: DSBnotes
  http://www.dsbnotes.de/
- Otris software AG: privacyGUARD
  https://www.privacyguard.de/privacyguard/de/home.jhtml
- Sicoda: DSBeasy
  http://www.sicoda.de/dsbeasy-verfahrensverzeichnis-software/
- WEKA Verlag: Verfahrensverzeichnis-Manager – Das Excel-Tool
  http://shop.weka.de/verfahrensverzeichnis-manager-das-excel-tool

Bitkom vertritt mehr als 2.300 Unternehmen der digitalen Wirtschaft, davon gut 1.500 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom