Das Verarbeitungsverzeichnis

Verzeichnis von Verarbeitungstätigkeiten
nach Art. 30 EU-Datenschutz-Grundverordnung
(DS-GVO)

www.bitkom.org

bitkom

Herausgeber

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

Ansprechpartner

Susanne Dehmel | Mitglied der Geschäftsleitung
T 030 27576-223 | s.dehmel@bitkom.org

Autoren

- Wolfgang Braun, Konzerndatenschutzbeauftragter Giesecke & Devrient GmbH
- Susanne Dehmel, Mitglied der Geschäftsleitung Bitkom e.V.
- Heiko Gossen, Geschäftsführender Gesellschafter migosens GmbH
- Bernd H. Harder, Harder Rechtsanwälte
- 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

Satz & Layout

Katrin Krause | Bitkom

Titelbild

© weerapat1003 – Fotolia.com

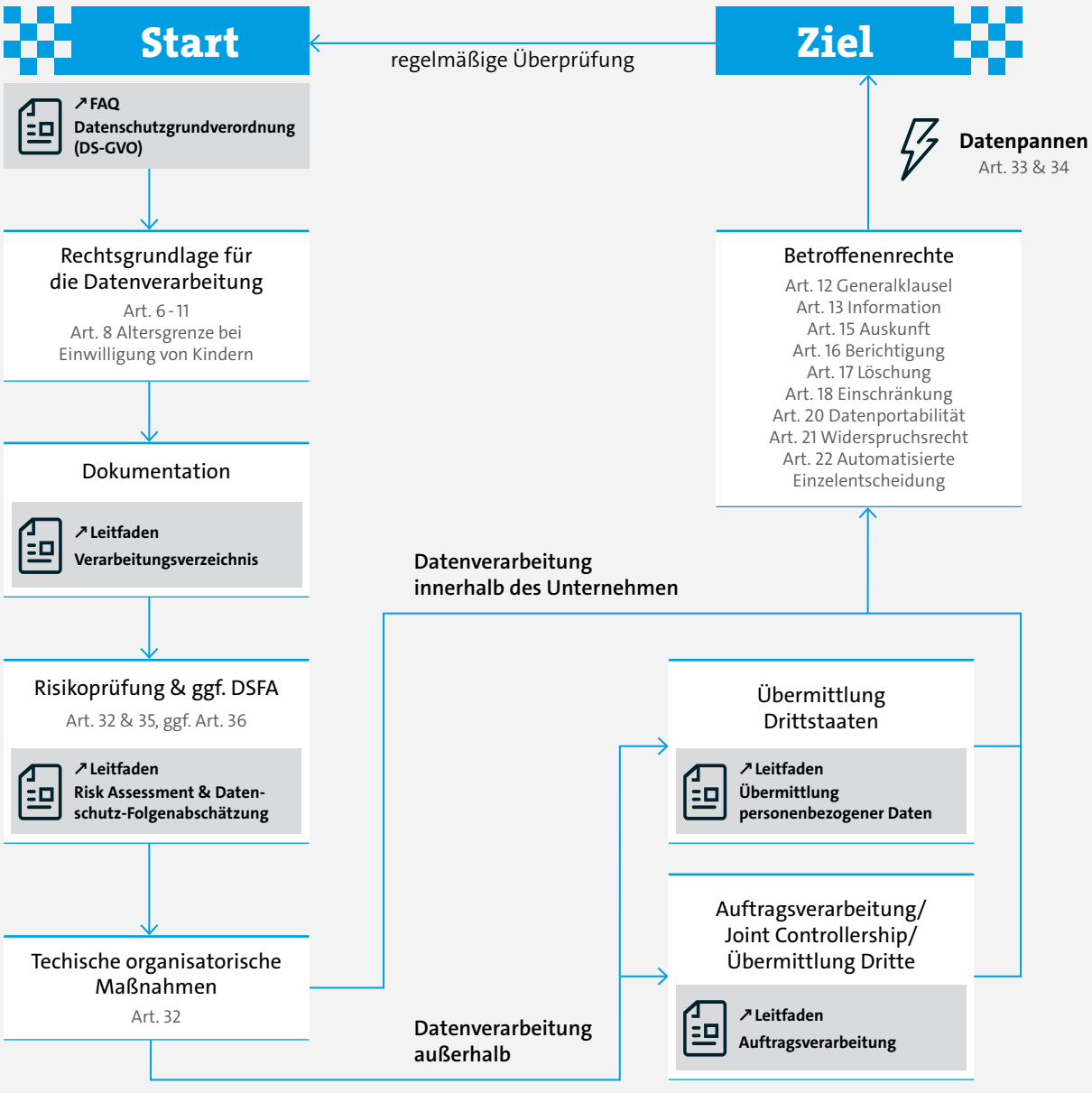
Das Verarbeitungsverzeichnis

Verzeichnis von Verarbeitungstätigkeiten
nach Art. 30 EU-Datenschutz-Grundverordnung
(DS-GVO)

Datenschutzkonforme Datenverarbeitung

nach der EU-Datenschutz-Grundverordnung (DS-GVO)*

Art. 5 Datenschutzprinzipien & Art. 25 Datenschutz durch Technikgestaltung



*alle Artikel sind solche der DS-GVO

bitkom

Inhaltsverzeichnis

Vorwort zur Version 4.0

Die letzte Handreichung zur Führung eines Verfahrensverzeichnisses (3.0), entsprechend den Vorgaben des BDSG, hat der Bitkom im Frühjahr 2016 veröffentlicht. Durch das Inkrafttreten der EU-Datenschutz-Grundverordnung (DS-GVO) im Mai 2016 und der Anwendbarkeit der neuen Regeln ab Mai 2018 werden die bisherigen BDSG Regelungen zur Führung eines Verfahrensverzeichnisses durch EU-weit geltende Vorgaben der Verordnung ersetzt. Dabei wird auch der Begriff Verfahrensverzeichnis durch den Begriff Verzeichnis der Verarbeitungstätigkeiten (oder kurz Verarbeitungsverzeichnis) abgelöst. Es entfällt die bisher bestehende allgemeine Meldepflicht nach § 4d Abs. 1 BDSG, während eine allgemeine Nachweis- und Dokumentationspflicht für die Rechtmäßigkeit der Verarbeitung bei der verantwortlichen Stelle verankert wird (Art. 24 Abs. 1 DS-GVO). Ebenfalls findet sich in der Verordnung die ausdrückliche Verpflichtung der verantwortlichen Stelle sowie (neu) der Auftragsverarbeiter zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten (Art. 30 DS-GVO). Ausgenommen sind hiervon lediglich Unternehmen mit weniger als 250 Mitarbeitern, die nur in beschränktem Umfang und unkritische Daten verarbeiten (Art. 30 Abs. 5 DS-GVO).

Die Dokumentation der Datenverarbeitungsprozesse im Unternehmen bleibt also eine wichtige Aufgabe und Grundlage für die rechtmäßige und rechtssichere Verarbeitung personenbezogener Daten. Dies gilt umso mehr angesichts der durch die DS-GVO enorm gestiegenen möglichen Bußgelder für Datenschutzverstöße. Sie kann aber nicht nur als Nachweis gegenüber den Aufsichtsbehörden dienen, sondern ebenso bei der Umsetzung und Überwachung sämtlicher sonstiger Pflichten der verantwortlichen Stelle gegenüber den Betroffenen (z.B. Informations- und Auskunftsrechte, Löschung) helfen. Für den Datenschutzbeauftragten des Unternehmens ist sie ein wichtiges Hilfsmittel bei der Erfüllung seiner Aufgaben. Daher empfiehlt sich die Auseinandersetzung mit dem Thema Verarbeitungsübersicht in jedem Fall – selbst wenn das eigene Unternehmen nicht nach der DS-GVO zur Führen einer solchen verpflichtet ist.

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
- Bernd H. Harder, Harder Rechtsanwälte
- 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 28. April 2017

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 Verarbeitungsverzeichnis ist eine Dokumentationsform und zentrales Instrument des Datenschutzrechts zur Umsetzung dieser Transparenzpflichten.

Der folgende Leitfaden erklärt Begriffe und Grundlagen des Verarbeitungsverzeichnisses 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 Verarbeitungsverzeichnis

2.1 Begriffsbestimmungen

Artikel 30 der EU Datenschutz-Grundverordnung (DS-GVO) verpflichtet Unternehmen zum Führen eines »Verzeichnisses von Verarbeitungstätigkeiten«. Im allgemeinen Sprachgebrauch hat sich die Kurzform »Verarbeitungsverzeichnis« in Anlehnung an den früher verwendeten Begriff des »Verfahrensverzeichnisses« etabliert.

Die bisherige Rechtslage unter dem BDSG (bis 25.5.2018) forderte bereits ein Verfahrensregister, das in Teilen sogar jedermann auf Antrag einsehen können musste. In der Praxis wurden oft unterschiedliche Begriffe für diese gesetzlich geforderte Dokumentation verwendet. In dem Vorgänger zu diesem Leitfaden wurde die zur öffentlichen Kenntnisnahme gedachte Dokumentation öffentliches Verfahrensverzeichnis genannt, in Praxis und Literatur auch als »Jedermannverzeichnis« oder Verfahrensregister beschrieben. Die DS-GVO sieht weder die Möglichkeit zur Einsichtnahme für Jedermann noch eine Meldepflicht der Verfahren für Unternehmen vor. Daher bedarf es begrifflich keiner Unterscheidung mehr zwischen »öffentlich« und »intern«. Allerdings ist der Aufsichtsbehörde das Verarbeitungsverzeichnis auf Anfrage zur Verfügung zu stellen.
Da, wie weiter unten beschrieben, das Verarbeitungsverzeichnis um einige sinnvolle Dokumentationen ergänzt werden kann, diese aber nicht zum gesetzlich vorgeschriebenen Teil der Verarbeitungsverzeichnisses gehören, wird hierfür im Weiteren der Begriff »erweitertes Verarbeitungsverzeichnis« verwendert.

Weitere etablierte Begriffe haben sich durch die DS-GVO leicht geändert, so spricht die Verordnung nunmehr statt von der »verantwortlichen Stelle« vom »Verantwortlichen« und statt »Auftragsdatenverarbeitung« heißt es nunmehr »Auftragsverarbeitung«. Entsprechend heißt der bisherige »Auftragnehmer« nun »Auftragsverarbeiter«.

2.2 Ziel und Zweck des Verarbeitungsverzeichnisses

Das Verarbeitungsverzeichnis 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. Der Verantwortliche oder der Auftragsverarbeiter stellen nach Art. 30 Abs. 4 DS-GVO das Verarbeitungsverzeichnis der Aufsichtsbehörde auf Anfrage zur Verfügung. Das Verarbeitungsverzeichnis dient gegenüber der Aufsichtsbehörde zum Nachweis, dass die Vorschriften der DS-GVO vom Verantwortlichen eingehalten wurden. Dies gehört zu der generellen Pflicht des Verantwortlichen, mit der Aufsichtbehörde bei der Erfüllung ihrer Aufgabe auf Anfrage zusammenzuarbeiten (Art. 31 DS-GVO).

Das Verarbeitungsverzeichnis ist somit gleichermaßen Grundlage zur Erfüllung unternehmerischer Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters und Hilfsmittel der Tätigkeit von deren Datenschutzbeauftragten.

2.3 Pflicht zur Führung eines Verarbeitungsverzeichnisses

Die Verpflichtung zur Führung eines Verarbeitungsverzeichnisses ergibt sich aus Art. 30 der Datenschutzgrundverordnung. Das Verzeichnis dient entsprechend Erwägungsgrund 82 zum Nachweis der Einhaltung der Verordnung.

Der Umfang der Dokumentation umfasst alle Verarbeitungstätigkeiten des Verantwortlichen.

Grundsätzlich unterliegt jeder Verantwortliche der Pflicht ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen und zu führen. Zwar sind zwei oder mehr Verantwortliche, die gemeinsam die Zwecke und Mittel zur Verarbeitung festlegen gemeinsam Verantwortliche (Joint Controllers). Allerdings muss nicht jeder von Ihnen ein Verzeichnis führen. Vielmehr legen sie in einer Vereinbarung fest, wer von ihnen welche Verpflichtung gemäß der DS-GVO erfüllt und somit das Verzeichnis erstellt und führt. Auch der Auftragsverarbeiter muss ein Verzeichnis führen, das alle Kategorien von Verarbeitungstätigkeiten enthält, die der Auftragnehmer im Auftrag eines Verantwortlichen durchführt.

Sofern der Verantwortliche oder der Auftragsverarbeiter nicht in der Union niedergelassen sind und einen Vertreter in der Union zu benennen haben, ist dieser Vertreter ebenfalls zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten verpflichtet.
Die Pflicht zum Führen des Verzeichnisses gilt nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen. Allerdings entfällt die Pflicht nur unter der Voraussetzung, dass die Verarbeitungen nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 eingeschlossen wird. Diese sehr kompliziert formulierte Ausnahme von der Ausnahme führt in der heutigen digitalen Welt vermutlich dazu, dass nur sehr wenige Unternehmen von der Pflicht zur Führung eines Verarbeitungsverzeichnisses ausgenommen sein dürften.

Der Verantwortliche oder der Auftragsverarbeiter, sowie gegebenfalls deren Vertreter, stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung. Eine Meldepflicht, die das Bundesdatenschutzgesetz bzw. die Datenschutzrichtlinie kannten, gibt es im Kontext der Datenschutzgrundverordnung nicht. Die Verpflichtung zur Verfügungstellung auf Anfrage konkretisiert, unter anderem, die Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde, die Art. 31 DS-GVO formuliert.

Das Führen des Verarbeitungsverzeichnisses ist eine ausgezeichnete Grundlage, um die notwendigen Informationen im Hinblick auf die Rechenschafts- und Dokumentationspflichten zusammenzustellen und verfügbar zu haben.

Zu den Rechenschaftspflichten, die die DS-GVO vorsieht, gehören:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Mit dem Verarbeitungsverzeichnis kann die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und die Freiheiten der betroffenen Person in Bezug auf Art, Umfang und Umstände sowie Zwecke der Verarbeitung im Rahmen der Datenschutz-Folgenabschätzung abgeleitet werden. Das Verarbeitungsverzeichnis dient zur Identifizierung der Rechtsmäßigkeit der Verarbeitungen, insbesondere im Hinblick auf erteilte Einwilligungen. Die Dokumentation der getroffenen technischen und organisatorischen Maßnahmen ist Bestandteil des Verzeichnisses und somit erste Quelle für die Beurteilung der Angemessenheit der Maßnahmen.

Alle diese Gründe sprechen für das Führen eines Verzeichnisses der Verarbeitungstätigkeiten, auch wenn das Unternehmen dazu nicht gesetzlich verpflichtet ist. Es ist für den Verantwortlichen und den Datenschutzbeauftragten eine nahezu unverzichtbare Sammlung aller Informationen zu den Verarbeitungen von personenbezogenen Daten.

2.4 Verantwortlichkeiten

Bei der Frage, wer das Verarbeitungsverzeichnis führt, muss zwischen der formalen Verantwortlichkeit einerseits und der praktischen Ausführung im Unternehmen andererseits unterschieden werden. Außerdem ist bei der Definition der Verarbeitungsaktivitäten zu berücksichtigen, ob eine Auftragsverarbeitung, eine gemeinsame Verantwortung (Joint controllership) oder eine Übermittlung an einen Dritten[1] vorliegt, da sich hier die Pflichtangaben je Verarbeitung unterscheiden.

2.4.1 Die Geschäftsführung

Die formale Verantwortlichkeit für die Erstellung und ordnungsgemäße Führung des Verarbeitungsverzeichnisses liegt bei der Unternehmensleitung des Verantwortlichen, bzw. Auftagsverarbeiters. Sie hat gemäß Artikel 30 Abs. 1 DS-GVO ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Gleichzeitig muss der Verantwortliche laut Artikel 38 DS-GVO sicherstellen, dass der Datenschutzbeauftragte frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird (Abs. 1) und er muss dem Datenschutzbeauftragten die erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbei-

1 Nähere Ausführungen zur Abgrenzung im Leitfaden »Begleitende Hinweise zur Mustervertragsanlage Auftragsverarbeitung«.

tungsvorgängen zur Verfügung stellen (Abs.2). Zwar übernimmt in der Praxis oftmals der Datenschutzbeauftragte die Führung des Verarbeitungssverzeichnisses, insbesondere die Erstellung der einzelnen Verfahrensmeldungen obliegt dabei jedoch der Fachabteilung und nicht dem Datenschutzbeauftragten. Der sollte auf die Erstellung hinwirken und Hilfestellung anbieten, aber keine Verantwortung für die Inhalte tragen. Die Verantwortung für die einzelnen Verfahren verbleibt bei den Fachabteilungen und letztlich bei der Leitung des Verantwortlichen.

Mit dem Begriff des Verantwortlichen 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 Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Diese Definition ergibt sich unmittelbar aus Art. 4 Abs. 7 DS-GVO. Für Unternehmen bedeutet dies, dass Verantwortlicher 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.

Jedes Unternehmen mit eigenständiger Rechtspersönlichkeit stellt grundsätzlich einen Verantwortlichen dar. Deshalb muss für jedes Unternehmen innerhalb des Konzerns und alle eigenständigen Tochterfirmen ein Verarbeitungsverzeichnis geführt werden. Anderes kann nur im Fall einer Joint Controllership gelten (↗s. unter 2.4.3.)

Merke

Im Grundsatz ist jedes rechtlich eigenständige Unternehmen ein Verantwortlicher im Sinne des Art. 4 DS-GVO.

2.4.2 Der Datenschutzbeauftragte

In der DS-GVO gibt es keinen expliziten Bezug zwischen dem Datenschutzbeauftragten und dem Verarbeitungsverzeichnis. Die Führung der Verarbeitungsübersicht gehört weder zu seinen vorgeschriebenen Aufgaben noch ist er dazu verpflichtet hierzu Vorgaben zu machen. In der betrieblichen Praxis hat es sich jedoch bewährt, auch die Anforderungen des Datenschutzbeauftragten bei der Erstellung und Führung des Verarbeitungsverzeichnisses zu berücksichtigen.

Führt der Datenschutzbeauftragte das Verarbeitungsverzeichnis 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 Gemeinsam Verantwortliche (Joint Controllership)

Die DS-GVO sieht in Artikel 26 die Möglichkeit vor, dass zwei Verantwortliche gemeinsam für eine oder mehrere Datenverarbeitungen verantwortlich sein könnnen. Voraussetzung ist, dass sie gemeinsam die Zwecke und Mittel zur Verarbeitung festlegen und in einer Vereinbarung die jeweiligen Pflichten verteilen[2]. In dieser Konstellation sollte auch festgelegt werden, wer für die Führung des Verarbeitungsverzeichnisses verantwortlich ist. Dieser Verantwortliche muss das Verarbeitungsverzeichnis führen und dort auch gemäß Art. 30 Abs. 1 a) DS-GVO den mit ihm gemeinsam Verantwortlichen aufführen.

2.4.4 Verantwortlichenkeiten bei Auftragsverarbeitung

Wenn ein Unternehmen einzelne Datenverarbeitungsprozesse oder auch seine gesamte Datenverarbeitung im Wege der Auftragsverarbeitung nach Artikel 28 DS-GVO auf einen Dienstleister überträgt, wie zum Beispiel im Rahmen von Outsourcing, ist die Frage zu klären, wer für welchen Teil der Dokumentation der Verarbeitung zuständig ist.

Anders als bisher im BDSG enthält die DS-GVO mit Art. 30 Abs. 2 eine eigene Vorschrift in Bezug auf die Verpflichtung des Auftragsverarbeiters zur Führung eines Verarbeitungsverzeichnisses. Darin wird er verpflichtet, ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätkgeiten der Verarbeitung zu führen. In Abs. 2 a)-d) ist aufgeführt, welche Inhalte dieses Verzeichnis aufweisen muss. Nach Art. 30 Abs. 4 muss der Auftragsverarbeiter das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung stellen.

Parallel dazu besteht jedoch bei dem beauftragenden Verantwortlichen die Verpflichtung aus Art. 30 Abs. 1 ein Verzeichnis aller Verarbeitungstätigkeiten zu führen, die ihrer Zuständigkeit unterliegen.

Dabei ist zu beachten, für welche Verfahren der Auftragsverarbeiter ggfs. selbst wiederum Verantwortlicher ist (bspw. bei den Verarbeitungen der Daten der eigenen Mitarbeiter), denn hierfür muss er die ↗unter 5.1 genannten Inhalte dokumentieren. In der Praxis wird er daher zwei Verzeichnisse führen: eines für seine eigenen Verarbeitungen als Verantwortlicher und eines für die Verarbeitungen als Auftragsverarbeiter für seine Kunden.

Die Inhalte, die jeweils im Verarbeitungsverzeichnis des Verantwortlichen und des Auftragsverarbeiters abgebildet werden, variieren entsprechend der jeweiligen Verantwortungssphäre von Verantwortlichem und Auftragsverarbeiter. Während der Verantwortliche den Zweck der Verarbeitung sowie die Kategorien der Daten und der Empfänger angeben muss, sind es beim Auftragsverarbeiter die Kategorien von im Auftrag durchgeführten Tätigkeiten der Verarbeitung (↗s.u. 2.5.1). Gemäß Art. 31 DS-GVO müssen sowohl der Verantwortliche als auch der Auftragsverarbeiter mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenarbeiten.

2 Näheres dazu in den Erläuterungen zur Mustervertragsanlage Auftragsverarbeitung und der Checkliste Joint Controllership.

2.4.5 Verantwortlicher oder Auftragsverarbeiter außerhalb der EU und Vertreter

Nicht-öffentliche Verantwortliche oder Auftragsverarbeiter außerhalb der EU, die Daten verarbeiten, auf die die DS-GVO Anwendung findet, müssen nach Art. 27 Abs. 1 einen Vertreter in der Union benennen, sofern ihre Datenverarbeitung mehr als gelegentlich erfolgt oder die Verarbeitung besonderer Kategorien personenbezogener Daten umfasst (Art. 27 Abs. 2 a) DS-GVO) und die Voraussetzungen des Art. 3 Abs. 2 DS-GVO vorliegen. Dieser Vertreter soll insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung zur Gewährleistung der Einhaltung der DS-GVO als Anlaufstelle dienen (Art. 27 Abs. 4). Nach Erwägungsgrund 80 sollte er im Namen des Verantwortlichen oder Auftragsverarbeiters tätig werden. Der Verantwortliche oder der Auftragsverarbeiter sollte den Vertreter dazu ausdrücklich bestellen und schriftlich beauftragen, in Bezug auf die ihm nach dieser Verordnung obliegenden Verpflichtungen an seiner Stelle zu handeln.

In Artikel 30 Abs. 1 wird der Vertreter erwähnt: »jeder Verantwortliche und gegebenenfalls (in der englischen Fassung: where applicable) sein Vertreter führen ein Verzeichnis aller Verarbeitungstätgkeiten, die ihrer Zuständigkeit unterliegen.« Insbesondere die englische Formulierung lässt darauf schließen, dass der Verordnungsgeber davon ausgeht, dass im Falle eines bestellten Vertreters dieser auch das Verarbeitungsverzeichnis für die ihm zugeordnetetn Verarbeitungen führt.[3]

Dies erscheint auch insoweit plausibel, als dass er im Zweifel derjenige sein wird, von dem die Aufsichtsbehörde die Vorlage des Verzeichnisses verlangen wird. Dies ist jedoch der einzige Hinweis in der Verordnung, dass der Vertreter derjenige sein soll, der das Verzeichnis führt. Es könnte theoretisch auch der Verantwortliche selbst sein, sofern sie sicherstellt, dass der Vertreter auf das Verzeichnis wenn nötig zugreifen kann.

2.5 Inhalt und Aufbau des Verarbeitungsverzeichnisses

Der beim Verantwortlichen mit der Führung des Verarbeitungsverzeichnisses Beauftragte[4] muss sich zu Beginn seiner Tätigkeit entscheiden, wie er das Verarbeitungsverzeichnis führt. Sein Vorgehen sollte sich am Aufbau und der Komplexität des Unternehmens orientieren. Der Detailgrad des Verarbeitungsverzeichnisses sollte sich auch an den Anforderungen des Datenschutzbeauftragten und dessen Arbeitsweise orientieren. Gleichzeitig muss das Verarbeitungsverzeichnis so ausgestaltet sein, dass es den gesetzlichen Anforderungen aus Art. 5 Abs. 2 (»Rechenschaftspflicht«) sowie den Art. 24 und 30 DS-GVO genügt. Um unnötige Doppeldokumentation zu ver-

3 Plath in Plath (Hrsg.), BDSG/DS-GVO, 2. Aufl. 2016, Art. 27 Rn 6 »Weiterhin ist der Vertreter zur Führung eines Verfahrensverzeichnisses nach Art. 30 Abs. 1 verpflichtet«.

4 Im Weiteren wird davon ausgegangen, dass der Datenschutzbeauftragte in vielen Fällen vom Verantwortlichen mit der Koordinierung und Führung des Verarbeitungsverzeichnisses beauftragt wird. Wird jemand anderes im Unternehmen hiermit beauftragt, kann der Prozess entsprechend adaptiert werden.

meiden, kann im Verarbeitungsverzeichnis auch auf bereits bestehende Dokumente z.B. mit dem allgemeinen Sicherheitskonzept bzw. den übergreifenden technischen und organisatorischen Maßnahmen verwiesen werden. Es ist jedoch zu beachten, dass diese im Bedarfsfall dann auch der Aufsichtsbehörde mit zur Verfügung gestellt werden müssen.

Verarbeitungsverzeichnis beim Veranwortlichen

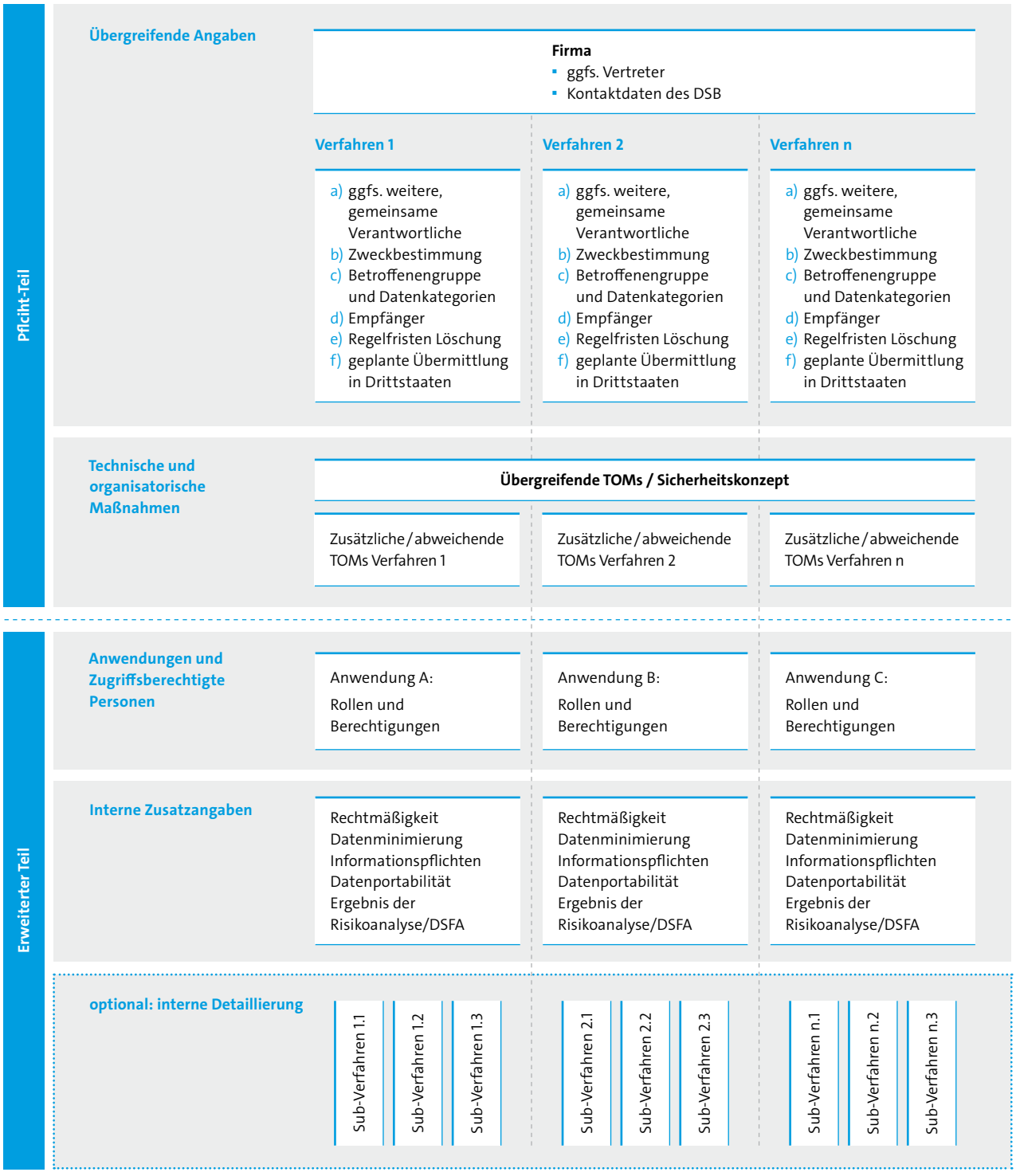


Abbildung 1: Verarbeitungsverzeichnis

2.5.1 Pflichtangaben im Verarbeitungsverzeichnis des Verantwortlichen

Gemäß Art. 30 Abs. 1 a) bis g) DS-GVO sind im Verarbeitungsverzeichnis des Verantwortlichen folgende Angaben zu machen:

Art. 30 Abs. 1	Inhalte	Erläuterung
a)	Name und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten	Diese Angaben dienen im Sinne des Transparenzgebots der zweifelsfreien Identifizierung des Verantwortlichen (Unternehmen o. Organisation) und der zuständigen Personen.
b)	Die Zwecke der Verarbeitung	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«.
c)	Eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten	Gemeint sind die Personengruppen, deren Daten in dem jeweiligen Verfahren verarbeitet werden, zum Beispiel »Mitarbeiter« oder »Kunden«. Beispiele für Kategorien von personenbezogenen Daten sind Stammdaten (z.B. Kontaktdaten), Bewegungsdaten, Nutzungsdaten, etc.
d)	Die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen	Es empfiehlt sich in der Regeln eine Benennung der natürlichen oder juristischen Personenen, Behörden, Einrichtungen oder anderen Stellen die Daten planmäßig erhalten sollen. Unabhängig davon, ob es sich um eine aktive Übertragung oder einen Direktzugriff des Empfängers auf die Verarbeitung handelt. Dies können interne und externe Stellen, sowie Dienstleister im Rahmen der Auftragsverarbeitung sein.
e)	Gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien	Bei Datenübermittlungen nach Art. 49 Absatz 1 Untersatz 2 handelt es sich um Übermittlungen die ausnahmsweise zulässig sind, obwohl weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt, noch geeignete Garantien nach Art. 46 bestehen.
f)	Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien	Das »wenn möglich« ist nicht optional zu verstehen, sondern so, dass eine Löschregel in dem jeweils möglichen Konkretisierungsgrad angegeben werden soll. In der Regel richtet sich die Löschung nach dem Zweck der Datenerhebung und -nutzung. Zu Löschen ist grundsätzlich unverzüglich nach Erfüllung des Zwecks. Ausnahmen ergeben sich insbesondere aus spezialgesetzlichen Aufbewahrungspflichten, zum Beispiel aus dem Steuerrecht oder sonstigen branchenspezifischen Rechtsvorschriften.

Art. 30 Abs. 1	Inhalte	Erläuterung
g)	Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.	Hier kann auf das allgemeine Sicherheitskonzept / übergreifende TOMs verwiesen werden, so dass nur Abweichungen davon für das jeweilige Verfahren extra aufgeführt werden müssen.Bei Verweis auf ein Referenzdokument müsste dieses der Aufsichtsbehörde ggf. ebenfalls vorgelegt werden.

2.5.2 Pflichtangaben im Verarbeitungsverzeichnis des Auftragsverarbeiters

Gemäß Art. 30 Abs. 2 a) bis d) DS-GVO sind im Verarbeitungsverzeichnis des Auftragsverarbeiters folgende Angaben zu machen:

Art. 30 Abs. 2	Inhalte	Erläuterung
a)	Den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten	Die Formulierung ist etwas unklar, kann jedoch wohl so verstanden werden, dass neben den Kontaktdaten des Auftragsverarbeiters selbst zumindest die Kontaktdaten der Verantwortlichen oder, sofern dem Auftragsverarbeiter diese nicht direkt bekannt sind (weil er z.B. nur das 3. Glied in einer Kette von mehreren Auftragsverarbeitern ist), die Kontaktdaten seiner direkten Auftraggeber.
b)	Die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden	Die Kategorien von Verarbeitungen entsprechen in den meisten Fällen wohl den generell angebotenen/vereinbarten Leistungen des Auftragsverarbeiters an seine Kunden und können zumeist aus der Vereinbarung zur Auftragsverarbeitung entnommen werden
c)	Gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien	Bei Datenübermittlungen nach Art. 49 Absatz 1 Untersatz 2 handelt es sich um Übermittlungen die ausnahmsweise zulässig sind, obwohl weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt, noch geeignete Garantien nach Art. 46 bestehen
d)	Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1	Hier kann auf das allgemeine Sicherheitskonzept / übergreifende TOMs verwiesen werden, so dass nur Abweichungen davon für das jeweilige Verfahren extra aufgeführt werden müssen. Bei Verweis auf ein Referenzdokument müsste dieses der Aufsichtsbehörde ggf. ebenfalls vorgelegt werden.

2.5.3 Interne Zusatzangaben im Verarbeitungsverzeichnis des Verantwortlichen

Unternehmensindividuell sollte entschieden werden, ob die Aufnahme von Zusatzinformationen sinnvoll ist, die anhand von Verfahren dokumentiert werden können. Dies kann sich bei Informationen anbieten, die das Unternehmen benötigt, um im Zweifelsfalle die Rechtmäßigkeit der Verarbeitung nachweisen zu können. Hierzu ist es nach Art. 5 Abs.2 und Art. 24 der DS-GVO verpflichtet. So bietet das Verarbeitungsverzeichnis eine Möglichkeit zur Umsetzung einer strukturierten Dokumentation, die an verschiedenen Stellen der DS-GVO erwartet wird und somit die Nachweispflichten gemäß Art. 5 Abs. 2 DS-GVO (zumindest die Teile, die je Verfahren dokumentiert werden können) zu erfüllen.

Artikel	Inhalte	Erläuterung
Art. 5 Abs.1 a **Art. 6**	Rechtmäßigkeit a) Rechtsgrundlage b) Berücksichtigung besonderer Kategorien pb Daten ggf. besondere Geheimnispflichten bestimmter MA (Sozialgeheimnis) c) Kompatibilität bei Zweckänderung d) Einhaltung der Anforderung an Einwilligung (bspw. Doku der Einw.-Klausel einschl. Historisierung und Prüfvermerk) e) Berücksichtigung von Widersprüchen (bspw. können diese überhaupt berücksichtigt werden, ggfs. Verweis auf Prozess) f) Automatisierte Entscheidung im Einzelfall	Neben der verpflichtenden Erfassung des Verarbeitungszwecks sollte zur Erfüllung der Rechenschaftpflichten gem. Art. 5 auch die Rechtsgrundlage mitsamt ggfs. erforderlicher Abwägungen, Einwilligungsklauseln und Prüfvermerken, ob bspw. die Anforderungen an Widerspruchsmöglichkeiten oder die automatisierte Einzelentscheidung berücksichtigt wurden.
Art. 5 Abs.1 c **Art. 25**	Datenminimierung Privacy by design Privacy by default	Dies kann bspw. durch einen Prüfvermerk des Datenschutzbeauftragten, ob diese Grundsätze nach seiner Einschätzung ausreichend berücksichtigt wurde, dokumentiert werden.
Art. 5 Abs.1 d **Art. 5 Abs.1 e**	Richtigkeit der Daten Speicherbegrenzung / Löschung oder Einschränkung der Verarbeitung	Dokumentation bspw. durch Referenz auf Maßnahmen, Prozesse, wie diese sichergestellt wird
Art. 12-14	Informations- und Benachrichtigungspflichten a) Vollständigkeit der Informationen b) Einhaltung der Fristen c) Formvorgaben	Es sollte je Verfahren dokumentiert werden, wo und wie den Informationspflichten jeweils nachgekommen wird. Dies kann bspw. durch Verweis auf Datenschutzhinweise, Vertragsbestandteile, Disclaimer in Formularen, bei Mitarbeiterdaten z.B. auch durch Verweise bei Erhebung auf intern bekanntgemachte Betriebsvereinbarung etc. erfolgen.
Art. 20	Datenportabilität	Es sollte erfasst werden, ob für dieses Verfahren ein Anspruch seitens des Betroffenen besteht, wenn ja für welche Datenkategorien (ggfs. einschließlich Begründung). Es sollte der Stand der Umsetzung bzw. geplante Maßnahmen erfasst werden.

Artikel	Inhalte	Erläuterung
Art. 32	Technische und organisatorische Maßnahmen a) Ergebnis der Risikobewertung b) Möglichkeiten der Pseudo- und Anonymisierung c) Datum der letzten Überprüfung der Risikoeinschätzung	Neben den allgemeinen Beschreibungen der technischen und organisatorischen Maßnahmen (siehe Pflichtangaben) kann für die interne Steuerung eine detaillierte Dokumentation sinnvoll sein.
Art. 35	Datenschutz-Folgenabschätzung a) Erforderlichkeit b) Ergebnis	Es sollte das Ergebnis der Prüfung, ob eine DSFA erforderlich ist oder nicht einschl. Begründung dokumentiert werden. Sofern eine DSFA durchgeführt werden muss, sollte die DSFA ausführlich dokumentiert werden (siehe Leitfaden Risikomanagement und DSFA und hierzu im Folgenden ↗unter Kapitel 3.1)

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

Es empfiehlt sich auch die Übersicht der Personen oder Gruppen, die Datenzugriff haben, in das erweiterte Verarbeitungsverzeichnis aufzunehmen.

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 Auftragsverarbeitung (sofern nicht aus Empfängern ersichtlich)
- Schnittstellen
- Sicherheitskonzepte
- verantwortliche Ansprechpartner in den Fachbereichen

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

2.5.4 Interne Zusatzangaben im Verarbeitungsverzeichnis des Auftragsverarbeiters

Aus Sicht des Auftragsverarbeiters bieten sich ebenfalls einige erweiterte Angaben an, die eine Nachweisführung und Sicherstellung der Einhaltung der Anforderungen sicherstellen.

Artikel	Inhalte	Erläuterung
Art. 28 Abs. 3	Weisungen des Auftraggebers	Je vielfältiger oder kundenindividueller das Leistungsspektrum eines Auftragsverarbeiters ist, kann eine zentrale Dokumentation der erteilten Weisungen sich als sehr sinnvoll erweisen. Werden die Weisungen (auch solche, die außerhalb des Vertrages erteilt werden) bereits gepflegt, aber ggfs. an unterschiedlichen Stellen, kann ein Verweis im erweiterten Verarbeitungsverzeichnis in der betrieblichen Praxis sehr hilfreich sein.
	Löschverfahren	Die eingesetzten Löschverfahren und die Aufnahmen eines Löschprotokolls in die Verarbeitungsdokumentation können sinnvolle Arbeitshilfen darstellen.
Art. 28 Abs. 2	Unterauftragsverhältnisse	Zur Sicherstellung der Einhaltung der Genehmigungs- und Mitteilungspflichten beim Einsatz von unterbeauftragten Auftragsverarbeitern sollten diese zur jeweilgen Verarbeitung zugeordnet werden und ergänzende Dokumente (z.B. Genehmigung durch den Verantwortlichen) dazu abgelegt werden.

2.6 Definition einer Verarbeitungstätigkeit

In der DS-GVO ist der Begriff Verarbeitungstätigkeit nicht näher erläutert. Eine »Verarbeitung« ist in Art. 4 als »Vorgang oder Vorgangsreihe im Zusammenhang mit personenbezogenen Daten« beschrieben, wie

- das Erheben,
- das Erfassen,
- die Organisation,
- das Ordnen,
- die Speicherung,
- die Anpassung oder Veränderung,
- das Auslesen,
- das Abfragen,
- die Verwendung,
- die Offenlegung durch Übermittlung,
- Verbreitung oder eine andere Form der Bereitstellung,
- den Abgleich oder die Verknüpfung,
- die Einschränkung,
- das Löschen oder
- die Vernichtung.

Die regelmäßige Verwendung des Begriffs »Verarbeitungstätigkeit« in der DS-GVO an verschiedenen Stellen legt nahe, dass dieser Begriff sehr weit gefasst ist. Nicht nur von den oben aufgeführten möglichen Verarbeitungsschritten, sondern auch bzgl. der Abgrenzung einer Verarbeitungstätigkeit von einer anderen.

Der Begriff »Verarbeitungstätigkeit« wird daher in diesem Leitfaden als die Gesamtheit an Verarbeitungen verstanden, mit deren Hilfe eine Zweckbestimmung oder ein Bündel zusammengehöriger Zweckbestimmungen realisiert wird. Eine Verarbeitungstätigkeit kann aus einer Vielzahl von DV-Programmen und Dateien bestehen. Wesentlich für die Bestimmung der Verarbeitungstätigkeit ist der verfolgte Zweck der Datenverarbeitung.

In der Praxis ist die Frage zu klären, was genau nun eine Verarbeitung ist sowie welche Verarbeitungen im Verarbeitungsverzeichnis geführt werden müssen.

Einen bewährten Ansatz bietet hierbei die Ausrichtung der Verfahren an:

- Geschäftsprozessen der verantwortlichen Stelle (unsere empfohlene Vorgehensweise, um u.a. eine überschaubare Anzahl von Verzeichniseinträgen zu erhalten)
- Verarbeitungszwecken
- Systemen; Hard- und Software

2.7 Form des Verarbeitungsverzeichnisses

Nach Art. 30 Abs. 3 DS-GVO ist das Verzeichnis schriftlich zu führen, was jedoch auch in einem elektronischen Format erfolgen kann.

Neben der Umsetzung als Papierformular oder elektronischauf Basis von Textverarbeitungs-, Tabellenkalkulations-, Datenbanksoftware, kommt auch der Einsatz von spezialisierten Softwareprogrammen in Betracht. Im Anhang ↗unter 5.4 findet sich eine Übersicht einiger Anbieter, die jedoch bisher nicht weiter bewertet wurden.

Bei der Auswahl 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.

3 Erstellen des Verarbeitungs-verzeichnisses

Die Erstellung des Verarbeitungsverzeichnisses fällt nicht in den Aufgabenbereich des Datenschutzbeauftragten, sondern ist vom Verantwortlichen selbst vorzunehmen (Artikel 30 DS-GVO). Der Datenschutzbeauftragte sollte jedoch regelmäßig hier eine Beratungsfunktion im Sinne des Artikels 39 Abs. 1 DS-GVO übernehmen, wonach er den Verantwortlichen in Hinblick auf alle Verarbeitungen über die Pflichten nach der Verordnung unterrichten und beraten soll. Aufgrund seiner Fachkenntnis wird der Datenschutzbeauftragte, wie bereits in der Vergangenheit oft betriebliche Praxis, derjenige sein, der von der Unternehmensleitung die notwendigen Kompetenzen zur Steuerung der Umsetzung und datenschutzrechtlichen Bewertung der einzelnen Verfahren zugewiesen bekommt.

Die Erstellung des Verzeichnisses durch den Verantwortlichen kann typischerweise in mehrere Phasen unterteilt werden. Es beginnt in der Regel mit einer Planungsphase, in der neben den Verantwortlichkeiten und benötigten Ressourcen auch die erforderlichen Methoden (z.B. zur Durchführung der Risikobewertung, der Sicherheitsmaßnahmen und der Datenschutz-Folgenabschätzung, siehe ↗Leitfaden Risikoanalyse/DSFA) und entsprechende Formulare / Vorlagen erstellt werden.

Grafische Darstellung der einzelnen Phasen als Überblick

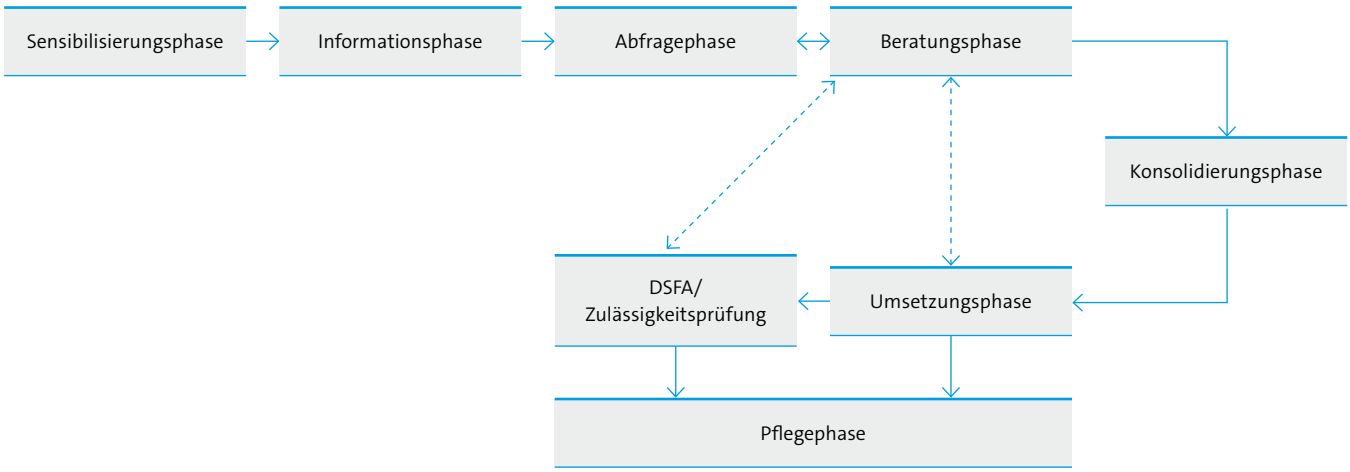


Abbildung 2: Grafische Darstellung der einzelnen Phasen als Überblick

3.1 Sensibilisierungsphase

In einem ersten Schritt sollten die Fachbereiche über die gesetzlichen Vorgaben zur Erstellung eines Verarbeitungssverzeichnisses und die damit verbundene Zielsetzung in Kenntnis gesetzt werden. Um dem Vorhaben die nötige Bedeutung beizumessen, sollte die Geschäftsführung als Verantwortlicher 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 Verarbeitungsverzeichnis aufgenommen werden müssen.

3.2 Informationsphase

Die von den Fachbereichen zu benennenden Mitarbeiter, die in die Erstellung des Verarbeitungsverzeichnisses 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 Datenschutz-Folgenabschätzung, damit alle Informationen rechtzeitig für die Datenschutz-Folgenabschätzung vorliegen (↗hierzu unter 3.7)

3.3 Abfragephase

Wie der betriebliche Datenschutzbeauftragte am effektivsten die notwendigen Informationen erhält, 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. Ist dies nicht der Fall, kann eine Fehlanzeige nach dem vorgegebenen Muster aufgenommen werden.

Es kann zweckmäßig sein, bereits bekannte (oder typischerweise in einem Unternehmen zu erwartende) Verarbeitungen im Rahmen eines Geschäftsprozesses schon vorab zu benennen und den Fachbereichen als Hilfestellung zur Verfügung zu stellen. Diese können dann, soweit möglich, eine Zuordnung ihrer Meldung zu diesen Verarbeitungen vornehmen. 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 Verarbeitungsverzeichnisses 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 sollten je nach Umfang und Komplexität auf die einzelnen Aufgabenbereiche verdichtet und inhaltlich konsolidiert werden, um das Verarbeitungsverzeichnis übersichtlich und handhabbar zu halten. Praktisch kann dies bedeuten, dass die einzelnen Verarbeitungsverzeichnisse 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 Verarbeitung im Verarbeitungsverzeichnis 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 Bedrohungen für die Rechte und Freiheiten der Betroffenen im Rahmen einer Riskoanalyse betrachtet und bewertet wurden und ob die Angaben über die technischen und organisatorischen Maßnahmen zum Schutz der Daten ausreichen. Kann dies anhand der vorhandenen Informationen nicht bestätigt werden, muss der Verantwortliche eine Risikoanalyse gem. Art. 32 DS-GVO durchführen (lassen) 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 Verarbeitungsverzeichnis 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 ob sie der Datenschutz-Folgenabschätzung unterliegen bzw. hiervon ausgenommen sind (Art. 35 Abs. 5 DS-GVO). Falls ja, ist ebenfalls erst eine Datenschutz-Folgenabschätzung durchzuführen, bevor die Verarbeitung freigeschaltet und im Verarbeitungsverzeichnis erfasst wird.

Ist sichergestellt, dass alle Informationen vollständig und richtig vorhanden sind, müssen diese als Verarbeitung im Verarbeitungsverzeichnis erfasst werden. Ob hierzu die Meldungen strukturiert in Papierform abgelegt oder elektronisch erfasst werden, kann von der verantwortlichen Stelle selbst festgelegt werden. Soll hierfür eine Software 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 Datenschutz-Folgenabschätzungund Zulässigkeitsprüfung

Zur Methodik siehe Leitfaden ↗»Risk Assessment und Datenschutz-Folgenabschätzung«.

Der Begriff der Datenschutz-Folgenabschätzung ist im Artikel 35 DS-GVO definiert und beschreibt die Pflicht des Unternehmens, bei bestimmten geplanten Datenverarbeitungen eine Datenschutz-Folgenabschätzung durchzuführen, bevor mit der Verarbeitung begonnen werden kann.. Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten ein (Art. 35 Abs. 2 DS-GVO). Damit kann der Datenschutzbeauftragte den Verantwortlichen und dessen Fachbereiche bei der Umsetzung der datenschutzrechtlichen Anforderungen beraten und die Zulässigkeit der Verarbeitung bewerten (Zulässigkeitsprüfung) bzw. bewerten, ob eine Datenschutz-Folgenabschätzung 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 Datenschutz-Folgenabschätzung, also der zwingenden Prüfung vor Beginn der Verarbeitung, unterliegen automatisierte Verarbeitungen, die aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, insbesondere bei Verwendung neuer Technologien (Art. 35 Abs. 1 DS-GVO). Um diese Datenschutz-Folgenabschätzung durchführen zu können, benötigt der Verantwortliche ein ordnungsgemäß erstelltes Verarbeitungsverzeichnis.). Die Eingaben sowie das Ergebnis der Datenschutz-Folgenabschätzung sollten nachvollziehbar dokumentiert werden und zu dem jeweiligen Verfahren referenziert abgelegt werden. Das Ergebnis kann auch Bestandteil des erweiterten Verarbeitungsverzeichnisses werden.

3.8 Pflegephase

Die Aktualisierung des Verarbeitungssverzeichnisses setzt eine permanente Kontaktpflege und Sensibilisierung der fachverantwortlichen Stellen zum Datenschutzbeauftragten voraus, der auf Meldungen zur Veränderung 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 Verarbeitungsverzeichnisses 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 Datenschutz-Folgenabschätzung nur bestätigen und bei der Durchführung beraten, 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 Software zur Führung des Verarbeitungsverzeichnisses

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

Im Folgenden eine Übersicht der grundsätzliche Funktionen, die jede Software bieten muss:
- Darstellung der nach Art. 30 DS-GVO 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 eine Software optional bieten sollte:
- Abbildung der beiden Rollen, des Verantwortlichen und des Auftragsverarbeiters
- 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 Verarbeitungsverzeichnisse

5.1.1 Beispiel für ein Verarbeitungsverzeichnis beim Verantwortlichen innerhalb der EU

Die folgenden Angaben sind die gesetzlich geforderten Mindestangaben, die auf Anforderung der Aufsichtsbehörde dieser zur Verfügung gestellt werden muss (Art. 30 Abs. 4 DS-GVO).

Name und Anschrift des Verantwortlichen	Datenschutzbeauftragter
Mustermann Marketing GmbH Eckstr. 5 60437 Frankfurt Tel: **+49 69 555-4514** E-Mail: info@mustermann-gmbh.de	**Herr Kraus** Datenschutzbeauftragter E-Mail: dsb@mustermann-gmbh.de Tel: **+49 69 555-4512**

Nr.	gemeinsam Verant-wortliche	Zweck	Betroffenengruppen	Datenkategorien	Empfänger	Übermittlung Drittstaaten	Löschfrist	Techn. u. organis. Maßnahmen
03	n.a.	Reisema-nagement	Beschäftigte	Buchungs- und Abrech-nungsdaten, Buchungs-präferenzen, Reisezeiten, Buchungshistorie, Legitimationsdaten (Kreditkartennr.)	Internes Reise-management, Reisebüro, Dienstleister Reiseserviceportal, Reisedienst-leister (Fluges, Bahn, Hotel), Visadienstleister, FiBu	bei Reisen in Drittländer oder Nutzung von Dienstleis-tern aus Drittländern	nach Ablauf von handels-, steuer-rechtlichen Aufbewahrungs-pflichten	Maßnahmen gemäß Sicher-heitskonzept, Schutzstufe normal Keine besonde-ren Maßnah-men gemäß Risikoanalyse erforderlich
04		Fuhrparkma-nagement	Leitende Mitarbeiter, Außendienstmitar-beiter	Stammdaten, Führer-scheindaten, Abrech-nungsdaten, Versiche-rungsdaten, Daten über besondere Vorgänge, Fahrzeugschäden, Unfall	internes Fuhr-parkmanage-ment oder externer Dienst-leister, Werkstatt und Servicepart-ner Versicherung	nicht geplant		
05		Marketing und Vertrieb	a) aktive und ehemalige Kunden b) Interessenten c) Webseiten-besucher	zu a & b: Kontakt- und Listendaten, Produktinter-essen, Kommunikations-historie, Bonitätsinforma-tionen zu a: Stammund Vertrags-daten Kaufhistorie 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 Kundenbezie-hung zu c: nach 6 Monaten durch Aggregation	

Nr.	gemeinsam Verant-wortliche	Zweck	Betroffenengruppen	Datenkategorien	Empfänger	Übermittlung Drittstaaten	Löschfrist	Techn. u. organis. Maßnahmen
06		Leistungser-bringung 1	a) Kunden b) ehemalige Kunden c) Beschäftigte d) Lieferanten	zu a & b: Stammdaten, Bestell- und Abrechnungs-daten zu c & d: Stammdaten, Leistungsnachweise			nach Ablauf von handels-, steuerrechtlichen Aufbewahrungs-pflichten	
07		Leistungser-bringung 2	a) Kunden b) ehemalige Kunden c) Beschäftigte d) Lieferanten	zu a & b: Stammdaten, Bestell- und Abrechnungs-daten zu c & d: Stammdaten, Leistungsnachweise			nach Ablauf von handels-, steuerrechtlichen Aufbewahrungs-pflichten	
08		Rechnungs-legung	a) Kunden b) ehemalige Kunden c) Beschäftigte d) Lieferanten	zu a & b: Stammdaten, Bestell-, Vertrags-, Abrech-nungs- und Zahlungsda-ten, Bankverbindungsda-ten zu c & d: Stammdaten, Leistungsnachweise	FiBu, Vertrieb, Support	nicht geplant	nach Ablauf von handels-, steuerrechtlichen Aufbewahrungs-pflichten	
09		Kundenbe-treuung	aktive und ehemali-ge Kunden	Stamm-, Vertrags- und Leistungsdaten, Abrech-nungsdaten, Korrespon-denz, Vorgangsinformatio-nen wie Support-Anfragen, Zahlungsausfälle etc.	FiBu, Vertrieb, Support	nicht geplant	nach Ablauf von Gewährleistungs- und Garantie-pflichten	
10		Beschaffung	Beschäftigte von Lieferanten	betriebliche Kontaktda-ten, ggf. Informationen über Kenntnisse und Fähigkeiten	Einkauf, Lager	nicht geplant; je nach Lieferant in Einzelfällen nicht ausge-schlossen	nach Ablauf von handels-, steuerrechtlichen Aufbewahrungs-pflichten	
11		Steuer- und handels-rechtliche Nachweis-erbringung, Finanzma-nagement	a) Kunden b) Lieferanten c) Beschäftigte d) Interessenten	Stammdaten, Leistungs- und Abrechnungsdaten	FiBu, Controlling	nicht geplant	nach Ablauf von handels-, steuerrechtlichen Aufbewahrungs-pflichten	
12		Unterneh-mens-, Objekt- und Informati-onssicher-heit	Beschäftigte, Kunden, Besucher	Stammdaten und Bilder für Firmenausweise, Berechtigungen, Accoun-tinformationen, Sicher-heitsprotokolle und Authentifizierungsdaten (Zutritt, Zugang, Zugriff, Weitergabe), Ergebnisse von Routinekontrollen, Besucherlisten, Raumbu-chungsinformationen, Videoüberwachungsbilder, Kennzeichen Privat-Kfz	Sicherheitsbe-auftragter, Empfang, ggfs. Rechtsabteilung		12 Monate nach Ablauf des Erhebungsjahres; 3 Jahre nach Beendigung des Beschäftigungs-verhältnisses	

5.1.2 Beispiel für ein Verarbeitungsverzeichnis beim Vertreter eines Verantwortlichen außerhalb der EU

Die folgenden Angaben sind die gesetzlich geforderten Mindestangaben, die auf Anforderung der Aufsichtsbehörde dieser zur Verfügung gestellt werden muss (Art. 30 Abs. 4 DS-GVO).

Name und Anschrift des Verantwortlichen	Vertreter innerhalb der Europäischen Union	Datenschutzbeauftragter
Mustermann Marketing Inc. 133 Ferry Morse Way Mountain View, CA 94041 USA **Tel: +1 555-4512-3453** E-Mail: info@mustermann.com	**Mustermann Marketing GmbH** Eckstr. 5 60437 Frankfurt **Standort Offenbach** Senefelderstr. 160 63069 Offenbach Geschäftsführer Frankfurt	**Herr Kraus** Datenschutzbeauftragter dsb@mustermann-gmbh.de **Tel: +49 69 555-4512**

Nr.	gemeinsam Verant-wortliche	Zweck	Betroffenengrup-pen	Datenkategorien	Empfänger	Übermittlung Drittstaaten	Löschfrist	Techn. u. organis. Maßnahmen
01	Muster-mann Vertriebs Inc. Muster-mann Datacenter Inc.	Bewerber-manage-ment	Bewerber	Stammdaten, Daten über Kenntnisse und Fähigkeiten wie Zeugnis-se, Lebenslauf, Beurtei-lungen, Kommunikati-onsdaten	Recruiting, Fachabteilung, FiBu, Mitbe-stimmungsgre-mien, Personal-dienstleister	USA	Bewerbungsunter-langen wie Zeugnisse, Lebenslauf etc.: 4 Monate nach Abschluss des Bewerbungsver-fahrens; mit Einwilligung des Betroffenen: 2 Jahre nach Eingang Bewer-bungsanschreiben, Korrespondenz: 10 Jahre	Maßnahmen gemäß Sicherheitskonzept, Schutzstufe 1
02	Muster-mann Vertriebs Inc. Muster-mann Datacenter Inc.	Personal-manage-ment	Beschäftigte i.S.d. § 3 Abs. 11 BDSG	a) Stamm- und Vertrags-daten b) Informationen über Kenntnisse und Fähigkeiten wie Zeugnisse, Lebenslauf und Beurteilungen c) Sozialversicherungs-daten, Abrechnungs-daten wie Lohndaten, Steuerklasse, Konfessi-onszugehörigkeit d) Bankverbindungsdaten e) Fehlzeiten	Personal, Fachabteilung, FiBu, Mitbe-stimmungsgre-mien, SV, FA, Bank	nicht geplant	3 Jahre nach Beendigung des Beschäftigungs-verhältnisses, nach Ablauf von handels-, steuer- und sozialversi-cherungsrechtli-chen Aufbewahrungs-pflichten	Maßnahmen gemäß Sicherheitskonzept, Schutzstufe 2 Ergänzend: Personal-abteilung gesonder-ter Zutrittsbereich

5.2 Beispiel für ein Verarbeitungsverzeichnis bei einem Auftragsverarbeiter

Der Auftragsverarbeiter muss ebenfalls ein Verarbeitungsverzeichnis führen, allerdings unterscheiden sich die zu dokumentierenden Pflichtinhalte.

Nachfolgend ein Beispiel für einen Dienstleister, der eine Bewerbermanagementlösung als Software as a Service (SaaS) anbietet:

Name und Anschrift des Auftragsverarbeiters[5]	Datenschutzbeauftragter
Mustermann Software GmbH Eckstr. 5 60437 Frankfurt Tel: **+49 69 555-4514** E-Mail: info@mustermann-gmbh.de **Standort Offenbach** Senefelderstr. 160 63069 Offenbach	**Herr Kraus** Datenschutzbeauftragter E-Mail: dsb@mustermann-gmbh.de Tel: **+49 69 555-4512**

Nr.	01
Verantwortlicher / Auftraggeber	Bernd Beispiel GmbH Kölner Str. 233 80999 München Tel: +49 89 555-9876 info@bernd-beispiel.de
Kategorien von Verarbeitungen	Abstrakte Beschreibung des Leistungsgegenstands oder der Leistungsgegenstände wie z.B. Bewerbermanagement in Form von SaaS oder Bereitstellung und Betrieb von Speicherkapazitäten
Übermittlung Drittstaaten	USA (Nutzung eines Cloud Infrastruktur-Anbieters) ▪ Beauftragung auf Basis von Standarddatenschutzklauseln gem. Art. 46 Abs.2 lit. c) DS-GVO[6]
Maßnahmen nach Art. 32 Abs. 1 DS-GVO	Maßnahmen gemäß internem Sicherheitskonzept + ggf. zusätzlich mit dem Auftraggeber vereinbarte spezielle Verschlüsselung2

5 Bei Sitz außerhalb der EU Umsetzung analog zu 5.1.2.

6 Angabe der angemessenen Garantie ist nur in bestimmten Fällen Pflicht, aber generell sinnvoll.

5.3 Formulare zur Erfassung der Verarbeitungsverzeichnisse

Die durchnummerierten Hinweise zu den Formularfeldern finden Sie ↗unter 5.3.4
Die Formulare werden auch als einzelne Word-Dateien ↗zum Download bereitgestellt.

5.3.1 Formular: Erfassung einer Verarbeitungstätigkeit

bitkom

Erfassung einer Verarbeitungstätigkeit

Seite 1|9

(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 der Verarbeitung (Hinweis Nr. 2):	< Text >
Übergeordneter Geschäftsprozess:	< Text >
Beginn der Verarbeitung (Hinweis Nr. 3):	< Text >

☐ **Änderung bestehende Verarbeitung**
☐ **neue Verarbeitung**
☐ **Abmeldung bestehende Verarbeitung (Hinweis Nr. 4)**

1. Grundsätzliche Angaben zur Verarbeitung und zur Verantwortlichkeit.

1.1 Bezeichnung des Verfahrens: (Hinweis Nr. 5)	< Text >
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 Auftragsverarbeitung nach Art. 28 DSG-VO (Hinweis Nr. 6):	< Text >
Vertrags-Nummer:	< Text >

www.bitkom.org

bitkom

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

2.1 Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung (Hinweis Nr. 8):
< Text >

2.2 Rechtsgrundlage (zutreffende bitte ankreuzen und erläutern)

☐ Spezialgesetzliche Regelung außerhalb der DSG-VO
(Bitte benennen: Vorschrift, Paragraph, Absatz, Satz)
< Text >

☐ Einwilligung des Betroffenen (Art. 6 Abs. 1 a) DSG-VO): Bitte fügen Sie die Einwilligungsklausel und den Einwilligungsmechanismus hier ein
< Text >

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

☐ Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (national geregelt im BDSG)
< Text >

☐ Vertrag oder Vertragsanbahnung mit dem Betroffenen
(Art. 6 Abs. 1 b) DSG-VO.)
< Text >

☐ Interessenabwägung (Art. 6 Abs. 1 f) DSG-VO):
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 Kategorien von Daten verarbeitet? (Hinweis Nr. 11)	
		☐ Ja Welche: < Text >	☐ Nein
		☐ Ja Welche: < Text >	☐ Nein
		☐ Ja Welche: < Text >	☐ Nein

bitkom

4. Datenweitergabe und deren Empfänger (Hinweis Nr. 12)

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 Konzern-unternehmen)

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. Mittel der Verarbeitung

Welche Software oder Systeme werden für diese Verarbeitung 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) Seite 4|9

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 (Art. 32 DSGVO) (Hinweis Nr. 15)

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

8.2 Es wurde eine Risikoanalyse gemäß Art. 32 DS-GVO durchgeführt.
☐ Ja
☐ Nein

8.3 Die Maßnahmen des allgemeinen Unternehmens-IT-Sicherheitskonzepts sind den festgestellten Risiken angemessen.
☐ Ja
☐ Nein

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

Verfügbarkeit	< Text >
Integrität	< Text >
Vertraulichkeit	< Text >
Weiterer Schutz der Rechte und Freiheiten der Betroffenen	< Text >

9. Datenübertragbarkeit (Hinweis 16)

Ist der Export der verarbeiteten Daten an den Betroffenen oder andere Dienste in einem gängigen, standardisierten Format möglich?

☐ Ja, Format: < Text >
☐ Nein

10. Information der Betroffenen (Hinweis 17)

Wie und wo werden den Betroffenen, deren Daten verarbeitet werden, die Pflichtinformationen über die Datenverarbeitung zugänglich gemacht?

< Text >

11. Datenschutz durch Technikgestaltung und Voreinstellungen (Hinweis 18)

Sind bei der Verarbeitung die Grundsätze des Datenschutz durch Technikgestaltung und der datenschutzfreundlichen Voreinstellungen eingehalten?

☐ Ja
☐ Nein

Anmerkungen:

< Text >

5.3.2 Formular: Meldung Fehlanzeige

bitkom

Fehlanzeige zur Erfassung von Verarbeitungstätigkeiten

Seite 1|2

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

Datum: < Text >

Grundsätzliche Angaben zur Verarbeitung und zur Verantwortlichkeit

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

☐ **Änderung bestehende Verarbeitung**
☐ **neue Verarbeitung**
☐ **Abmeldung bestehende Verarbeitung**

4. Fachbereich: < Text >
   Verantwortliche Führungskraft: < Text >
   ggf. Stellen-Kennzeichen: < Text >
5. Beschreibung der verarbeiteten Daten einschließlich Zweck der Verarbeitung: < 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 Verarbeitungsverzeichnis erforderlich	☐ Ja	☐ Nein
3. Datenschutzfolgeabschätzung erforderlich	☐ Ja	☐ Nein
4. Falls Datenschutzfolgeabschätzung erforderlich:	Ergebnis der Zulässigkeitsprüfung: ☐ Ja ☐ Nein	Anmerkungen: < Text >
5. Konsultation der Aufsichtsbehörde erforderlich:	< Text >	< Text >
6. 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 Erläuterungen zu den Formularen

Hinweis Nr. 1

»Personenbezogene Daten« sind nach Art. 4 Nr.1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden »betroffene Person«) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, Dies umfasst 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 der einzelnen Verarbeitung ermöglicht unter Zuordnung zum jeweiligen Geschäftsprozess, in dem die Daten verarbeitet werden.

Hinweis Nr. 3

Geplanter Beginn der Verarbeitung von personenbezogenen Daten oder tatsächlicher Beginn. Dabei ist schon die erstmalige Übertragung oder Speicherung von Daten relevant.

Hinweis Nr. 4

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

Hinweis Nr. 5

Genaue Kennzeichnung der Verarbeitung 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 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 und der Datenverarbeitung selbst. Es empfiehlt sich, entsprechende Erläuterungen möglichst unter der im Unternehmen bekannten Terminologie zu formulieren und in Zweifelsfällen Rücksprache mit dem Datenschutzbeauftragten zu halten.

Hinweis Nr. 9

Nennung der durch die Verarbeitung betroffenen 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

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist in Art. 9 Abs. 1 DS-GVO geregelt. Umfasst sind Verarbeitungen von Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

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, Auftragsverarbeiter (z. B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter), oder ein Verfahren, bzw. Geschäftsprozess, an den Daten weitergegeben werden.

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 Art. 5 Abs. 1 e) DS-GVO dürfen personenbezogene Daten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich 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 betrieblichen Datenschutzbeauftragten 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. Nähere Ausführungen zu den Anforderungen an Schutzmaßnahmen nach Art. 32 DS-GVO finden sich im Leitfaden Risk Assessment und Datenschutz-Fol-

genabschätzung im Kapitel 4.1. 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).

Hinweis Nr. 16

Bei Verarbeitungen auf Grundlage eines Vertrages oder einer Einwilligung, für die die Betroffenen dem Unternehmen Daten bereitgestellt haben, haben sie nach Art. 20 DS-GVO das Recht, diese sie betreffenden personenbezogenen Daten, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder sie an einen anderen Verantwortlichen übermitteln zu lassen, sofern dies technisch machbar ist.

Hinweis Nr. 17

Nach Art. 12 der DS-GVO müssen beim Verantwortlichen geeignete Maßnahmen getroffen werden, um den Betroffenen die in Art. 13 und 14 DS-GVO aufgeführten Angaben, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Dies kann schriftlich oder in einer anderen Form, z.B. elektronisch erfolgen.

Hinweis 18

Nach Art. 25 der DS-GVO müssen geeignete Mittel für die Verarbeitung festgelegt sowie technische und organisatorische Maßnahmen getroffen werden, die dazu ausgelegt sind, die Datenschutzvorgaben aus der Datenschutzverordnung wirksam umzusetzen und die Rechte der Betroffenen Personen zu schützen.

5.4 Anbieter von Software zur Erstellung des Verarbeitungsverzeichnisses

Stand: 29.05.2018

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

Verarbeitungsverzeichnis

2b Advice, Datenschutzsoftware:
↗https://www.2b-advice.com/GmbH-de/Datenschutzsoftware
(Es ist bereits mit der aktuellen Version möglich, alle Aspekte der DS-GVO abzubilden. Eine Version, die dann auch vom Wording und den voreingestellten Inhalten her nach DS-GVO ‚aussieht', befindet sich in den letzten Zügen der Fertigstellung und wird kurzfristig erscheinen, inklusive einem expliziten Modul für das Management von Datenschutzrisiken zur Folgenabschätzung)

Deichmann+Fuchs Business Solutions: DS-GVO – Verzeichnis der wichtigen Verarbeitungstätigkeiten
↗https://www.deichmann-fuchs.de/datenschutz/dsgvo-%E2%80%93-verzeichnis-der-wichtigen-verarbeitungst%C3%A4tigkeiten/dsgvo-verzeichnis-der-wichtigen-verarbeitungstaetigkeiten.artikel.html

d.velop GDPR compliance center:
↗https://store.d-velop.de/erweiterungen/d.velop-gdpr-compliance-center-/

GDPR-notes:
↗https://www.gdprnotes.de/en/ (im Aufbau)

Otris Privacy Konzerndatenschutz, Datenschutzmanagement-Software:
↗https://www.otris.de/produkte/otris-privacy-datenschutzmanagement/

Sicoda: DSBeasy Verfahrensverzeichnis Software:
↗https://www.sicoda.de/dsbeasy-verfahrensverzeichnis-software/
(unterstützt nach Angaben des Anbieters Anforderungen der DS-GVO)

WEKA, Datenschutz-Management kompakt:
↗https://shop.weka.de/datenschutz/datenschutz-management-kompakt

Bitkom vertritt mehr als 2.600 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