Verfahrensverzeichnis

und

Verarbeitungsübersicht

nach
BDSG

-Ein Praxisleitfaden-

Version 2.0

Redaktion: Dr. Kai Kuhlmann
Redaktionsassistenz: Karen Schlaberg
V.i.S.d.P.: Dr. Bernhard Rohleder

Inhaltsverzeichnis

Vorwort…… 6

Vorwort zur Version 2.0 6

Einführung…....8

Teil 1) Der Zusammenhang von Meldepflicht und Verfahrensverzeichnis 9

Teil 2) Verarbeitungsübersicht und Verfahrensverzeichnis....10

2 a) Verarbeitungsübersicht 10

2 b) Verfahrensverzeichnis....10

2 c) Wer muss das Verfahrensverzeichnis führen? 11

2c aa) Verantwortliche Stelle 11

2 c bb) Wer muss im Unternehmen das Verfahrensverzeichnis führen?.....11

2 c cc) Auftragsdatenverarbeitung und Funktionsübertragung 11

2 d) Inhalt und Form des Verfahrensverzeichnisses 12

2 e) Wer trägt im Unternehmen die Verantwortung für die Verarbeitungsübersicht? 13

2 f) Form der Verarbeitungsübersicht 13

2 g) Inhalte der Verarbeitungsübersicht....14

Teil 3) Wie kann eine Verarbeitungsübersicht erstellt werden? 16

3 a) Verknüpfung der Erstellung mit anderen unternehmensinternen Organisations- und Erfassungsprozessen 16

3 b) Frühzeitige Einbindung des Datenschutzbeauftragten....16

3 c) Die Erstellung der Verarbeitungsübersicht 18

3 c aa) Sensibilisierungsphase 18

3 c bb) Informationsphase 19

3 c cc) Abfragephase 19

3 c dd) Klärungsphase 19

3 c ee) Bearbeitungsphase 20

3 c ff) Pflegephase 20

Teil 4) Beispiele für Programmtools für die Erstellung des Verfahrensverzeichnisses ... 21

4 a) „BDSG Basics“ (Version 1.05.0) 21

4 b) „DPROREG Verfahrensverzeichnis“ (Version 2.1) 23

4 c) „DSBbrain 2000“ (Version 1.3.5) 24

4 e) „EMaVLight“ 25

Teil 5) Anhang 27

Anlage 1: Verpflichtung einen Datenschutzbeauftragten zu bestellen 28

Anlage 2: Übersicht zu Meldepflicht, Bestellung,Verfahrensverzeichnis und Verarbeitungsübersicht 29

Anlage 3: Beispiel Verfahrensverzeichnis 31

Anlage 4: Verfahren 33

Anlage 5: Formulare zur Verarbeitungsübersicht 35

5.1 Formular „Fehlanzeige“ 36

5.2 Formular „Meldung einer automatisierten Verarbeitung“ 37

5.3 Formular “Interner Prüfvermerk des Datenschutzbeauftragten“ 40

Anlage 6: Erläuterungen zu den Formularen 5.1 – 5.3 41

Teil 6: English Summary: Data Privacy Application Registration 44

6 a) Preamble 44

6 b) Who is responsible? 44

6 c) What is the minimum content of the application register? 44

6 d) What are the steps to establish an application register? 45

Profil …… 46

Vorwort

Der Praxisleitfaden „Verfahrensverzeichnis und Verarbeitungsübersicht nach BDSG“ ist eine Publikation des BITKOM – Arbeitskreises Datenschutz. Der Arbeitskreis besteht aus Experten der BITKOM - Mitgliedsfirmen und befasst sich mit aktuellen Themen und datenschutzspezifischen Aspekten der Informations- und Kommunikationstechnik. Ein Profil des Arbeitskreises befindet sich am Ende des Leitfadens.

Besonderer Dank gilt folgenden Mitgliedern des Arbeitskreises Datenschutz, die mit ihrer Expertise und wertvollen praktischen Erfahrung ganz maßgeblich zur Entstehung des Leitfadens beigetragen haben:

- Volker Ahrend, Konzerndatenschutzbeauftragter der Avaya GmbH & Co. KG
- Michael Bock, Rechtsanwalt, Team Manager Privacy and Security, E-Plus Mobilfunk GmbH & Co. KG
- Jörg Frahm, Datenschutzbeauftragter der Panasonic Marketing Europe GmbH und Panasonic Europe Ltd.

Berlin, den 19. April 2006

Vorwort zur Version 2.0

Verfahrensverzeichnis und Verarbeitungsübersicht sind weiterhin für die Praxis der betrieblichen Datenschutzbeauftragten ein wichtiges Feld. Wegen des stetigen Interesses an dem Leitfaden und der ausgesprochen positiven Resonanz der Leser wurde die im Frühjahr erschienene Version 1.0 zur vorliegenden Version 2.0 aktualisiert.

Berücksichtigt wurden dabei insbesondere die Änderungen im Bundesdatenschutzgesetz aufgrund des „Ersten Gesetzes zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft“ (vom 22. August 2006, BGBl. I, S.1970), das am 26. August 2006 in Kraft getreten ist. Diese Änderungen betreffen u. a. die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten, die Meldepflicht und die Bestellung externer Datenschutzbeauftragter bei Berufsgeheimnisträgern.

Berlin, den 10. Januar 2007

Jetzt mit Management-Summary & Anlagen auf Englisch!

Als weitere Publikationen des Arbeitskreises Datenschutz sind erhältlich:

- Leitfaden zur Nutzung von Email und Internet im Unternehmen (Version 1.4)
- Mustervertragsanlage zur Auftragsdatenverarbeitung (Version 2.0)
- Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer

Einführung

Datenschutz gehört zu den Kernaufgaben einer guten Geschäftsführung. Durch das Bundesdatenschutzgesetz werden heute an den betrieblichen Datenschutz klare Anforderungen bezüglich der Einhaltung des Datenschutzes und der Datensicherung gestellt. So sieht das Bundesdatenschutzgesetz (BDSG) z. B. eine laufende Überwachung der Rechtmäßigkeit aller Datenverarbeitungsvorgänge und eine Dokumentation der Datenhaltung ebenso vor wie ein funktionierendes Backup und einen Schutz von personenbezogenen Daten vor unbefugten Zugriffen.

Diese Anforderungen können insbesondere in größeren Unternehmen nur dann angemessen erfüllt werden, wenn ein sinnvolles Datenschutz- und Sicherheitsmanagement eingeführt wird (vgl. z.B. IT-Grundschutz etc.). Die Basis eines gesetzeskonformen Datenschutzmanagements ist die Erstellung des sog. Verfahrensverzeichnisses, denn der betriebliche Datenschutzbeauftragte (bDSB) muss sich als Voraussetzung seiner Arbeit einen umfassenden Überblick über die Struktur der im Betrieb eingesetzten Datenverarbeitungshardware und –software verschaffen. Erst die Bestandsaufnahme der eingesetzten IT-Systeme und vorhandenen Geschäftsprozesse bzw. automatisierten Verarbeitungen ermöglicht eine Gesamtbetrachtung und die Sicherung der Gesetzeskonformität aller Datenverarbeitungsvorgänge.

Ein effizient angelegtes Verfahrensverzeichnis kann zur **Kostenreduzierung** bei der Erfüllung der datenschutzrechtlichen Anforderungen erheblich beitragen. Zudem hat es wertvolle **Synergieeffekte** z.B. mit dem Bereich IT-Sicherheit und Risikomanagement.

Zielsetzung des Verfahrensverzeichnisses ist es, eine Dokumentation zu erstellen, die darüber Auskunft gibt,

- welche personenbezogenen Daten
- unter Verwendung welcher automatisierten Verfahren
- auf welche Weise verarbeitet oder genutzt werden und
- welche Datenschutzmaßnahmen durchgeführt werden.

Mit dem Verzeichnis soll sowohl innerhalb der verantwortlichen Organisation als auch (auf Antrag) für externe Personen und Stellen Transparenz bei der Verarbeitung personenbezogener Daten geschaffen werden. Verbessert werden soll damit auch die Auskunftsfähigkeit gegenüber Betroffenen und gegenüber den Aufsichtsbehörden, denen das Verzeichnis im Rahmen ihrer Beratungsbesuche und Überprüfungen zur Orientierung dienen kann.

Nicht zuletzt dient ein Verfahrensverzeichnis auch der rechtlichen Absicherung des Unternehmens. Mittlerweile gibt es Rechtsprechung, nach welcher die Verarbeitung personenbezogener Daten rechtswidrig sein kann, wenn eine gesetzlich erforderliche Vorabkontrolle nicht durchgeführt werden konnte, weil das Unternehmen kein ordnungsgemäßes Verfahrensverzeichnis führt (vgl. *VG Gießen*, RDV 2004, S. 257). Die rechtmäßige Verarbeitung personenbezogener Daten setzt daher ein ordnungsgemäß erstelltes Verfahrensverzeichnis voraus.

Teil 1) Der Zusammenhang von Meldepflicht und Verfahrensverzeichnis

Das **Bundesdatenschutzgesetz (BDSG)** geht im **Grundsatz** von **der Meldepflicht** aus: Unternehmen sind verpflichtet, "automatisierte Verarbeitungen" bei der Aufsichtsbehörde anzumelden, bevor sie diese in Betrieb nehmen, § 4d Abs. 1 BDSG. Welche Angaben zur Erfüllung dieser Meldepflicht zu machen sind, ergibt sich aus § 4e Satz 1 BDSG. Die Aufsichtsbehörde führt diese Angaben in einem für jedermann einsehbaren Verzeichnis.

Diese gesetzliche Meldepflicht **entfällt** jedoch, wenn – wie es in der Praxis häufig der Fall ist- das Unternehmen einen betrieblichen Datenschutzbeauftragten bestellt hat. Die Angaben aus § 4 e Satz 1 BDSG muss das Unternehmen gleichwohl erheben und dokumentieren. Die Aufgabe, ein Verzeichnis zu führen, fällt nämlich jetzt dem Unternehmen selbst zu. Das Bundesdatenschutzgesetz konkretisiert dies durch § 4 g Abs. 2 iVm § 4 d Abs. 2 BDSG, der bestimmt, dass die Meldepflicht für automatisierte Verfahren von den Unternehmen in Form eines Verfahrensverzeichnisses umzusetzen ist.

Zur Frage, welche Unternehmen verpflichtet sind, einen Beauftragten für den Datenschutz zu **bestellen**, siehe im Anhang Anlage 1.

Für die Praxis stellt sich damit zunächst die Frage:

Welche Unternehmen sind betroffen, d.h. welche Unternehmen müssen ein Verzeichnis führen?

Alle Unternehmen, die der gesetzlichen Meldepflicht unterliegen, müssen ein Verfahrensverzeichnis führen.

Durch den neu eingefügten § 4 g Abs. 2 a wird die vorher gesetzlich nicht eindeutig erfasste Frage beantwortet, ob auch diejenigen Unternehmen ein Verfahrensverzeichnis führen müssen, bei denen die Meldepflicht entfällt, da sie die Schwelle von neun Personen, die mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind, nicht überschreiten (§ 4 d Abs. 3 BDSG) und entweder eine Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient. Ist dies der Fall, trifft die Verpflichtung, eine Übersicht über die in § 4 e Satz 1 genannten Angaben zur Verfügung zu stellen laut § 4 g Abs. 2a BDSG den Leiter der verantwortlichen Stelle. Das hat zur Folge, dass **zumindest die Pflicht,** eine **Übersicht über die in § 4 e Satz 1 Nr. 1 bis 8 BDSG** genannten Angaben zu führen (Verfahrensverzeichnis), **auch dann besteht, wenn keine Meldepflicht besteht.**

Der Regelung lässt sich jedoch nicht entnehmen, ob auch eine **Verarbeitungsübersicht**[1] zu führen ist, wenn weder eine Meldepflicht, noch eine Verpflichtung besteht, einen Datenschutzbeauftragten zu bestellen (vgl. § 4 g Abs. 2 Satz 1).

Die Meldepflicht im europäischen Kontext

Die im BDSG statuierte Meldepflicht setzt die Vorgaben der **europäischen Datenschutzrichtlinie** um. Die Richtlinie 95/46/EG des Europäischen Parlaments vom 23.10.1995 (EU-DatSchRL) regelt in Abschnitt 9 die Meldung und die Vorabkontrolle. Die Pflicht zur Meldung bei einer Kontrollstelle ist in Artikel 18 geregelt, der davon ausgeht, dass die Meldepflicht die Meldung einer vollständig oder teilweise automatisierten Verarbeitung oder einer Mehrzahl

[1] Zu den Begrifflichkeiten vgl. Teil 2 unter 2 a)

von Verarbeitungen personenbezogener Daten für eine oder mehrere bestimmbarer Zwecke erfasst. Die Meldung soll dabei gegenüber einer zentralen Stelle erfolgen. Diese zentrale Stelle kann durch die Bestellung eines Datenschutzbeauftragten ersetzt werden, der als interne Kontrollstelle fungiert.

Aus dieser Zielrichtung der Meldepflicht der EU-Richtlinie lässt sich ableiten, dass für **internationale Unternehmen** eine **einheitliche Handhabung ratsam und sinnvoll** ist, insbesondere durch die Vereinheitlichung der Verfahrensverzeichnisse der Tochterunternehmen in den verschiedenen Ländern.

Teil 2) Verarbeitungsübersicht und Verfahrensverzeichnis

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 miteinander verbundenen Zweckbestimmungen realisiert wird. Ein Verfahren kann aus einer Vielzahl von DV-Programmen und Dateien bestehen, wesentlich für die Bestimmung des Verfahrens ist die definierte Aufgabe der Datenverarbeitung.

Es gibt unterschiedliche Bezeichnungen für die Teile der Verfahrensbeschreibungen, die das BDSG fordert. Mittlerweile hat sich hierfür überwiegend die Unterscheidung zwischen der Verarbeitungsübersicht und dem Verfahrensverzeichnis durchgesetzt, deren Struktur, Zweck und Inhalt im Folgenden erläutert werden.

2 a) Verarbeitungsübersicht

Die **Verarbeitungsübersicht** findet ihre gesetzliche Grundlage in § 4g Abs. 2 Satz 1 BDSG*: „Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen.“* Die Verarbeitungsübersicht dient der betriebsinternen Selbstkontrolle. Sie ist die Grundlage des betrieblichen Datenschutzbeauftragten für seine vielfältigen gesetzlichen Prüf- und Kontrolltätigkeiten. Zu diesem Zweck enthält sie die im Gesetz zwingend vorgegebenen Mindestinformationen.

2 b) Verfahrensverzeichnis

Das **Verfahrensverzeichnis** (häufig auch „**Jedermannverzeichnis**“ genannt) beruht auf § 4 g Abs. 2 Satz 3 BDSG, der bestimmt, dass der betriebliche Datenschutzbeauftragte die zur Erfüllung der Meldepflicht erforderlichen Angaben nach § 4 e Satz 1 Nr. 1 bis 8 BDSG *„auf Antrag jedermann in geeigneter Weise verfügbar“* macht. Im Gegensatz zur Verarbeitungsübersicht dient es also der Transparenz von unternehmensinternen Datenverarbeitungsprozessen gegenüber Dritten. Der Anspruch des Dritten auf Informationen aus dem Verfahrensverzeichnis besteht dabei neben dem Auskunftsanspruch des Betroffenen nach § 34 BDSG.

Die Verarbeitungsübersicht und das Verfahrensverzeichnis sind wesentliche Grundlagen und Teile der unternehmensinternen Datenschutzorganisation.

Nach seinem Sinn und Zweck geht das Gesetz wohl von dem Leitbild aus, dass aus der Verarbeitungsübersicht das Verfahrensverzeichnis erstellt wird. Die Erstellung der Verarbeitungsübersicht und des Verfahrensverzeichnisses müssen jedoch nicht zwingend aufeinander aufbauen. In der Praxis wird häufig zuerst ein sehr generisch gehaltenes Verfahrensverzeichnis erstellt, bevor der wesentlich komplexere Vorgang der Erstellung der Verarbeitungsübersicht begonnen wird, denn für die Erstellung des Verfahrensverzeichnisses ist die interne Erfassung der Verarbeitungen keine zwingende Voraussetzung. Auch diese Vorgehensweise entspricht den gesetzlichen Anforderungen. Da das Verfahrensverzeichnis jedoch keine detaillierten Rückschlüsse auf die internen Prozesse zulässt, ist letztlich immer auch eine Verarbeitungsübersicht notwendig.

2 c) Wer muss das Verfahrensverzeichnis führen?

Bei der Frage, wer das Verfahrensverzeichnis führt, muss zwischen der formalen Verantwortlichkeit einerseits und der praktischen Ausführung im Unternehmen andererseits unterschieden werden.

2c aa) Verantwortliche Stelle

Die formale Verantwortlichkeit für die ordnungsgemäße Führung des Verzeichnisses legt das BDSG der **verantwortlichen Stelle** auf. Mit dem Begriff der verantwortlichen Stelle ist die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle gemeint, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (so die Definition in Art. 2 der europäische Datenschutzrichtlinie). Für **Unternehmen** bedeutet das, dass die verantwortliche Stelle daher nicht diejenige Organisationseinheit (Abteilung, Dezernat, Referat, Zweigstelle) eines Unternehmens ist, die die Daten tatsächlich speichert bzw. verarbeitet (z.B. das Rechenzentrum oder die Personalabteilung), sondern **immer die übergeordnete juristische Person** (z. B. GmbH), der diese Organisationseinheit angehört. Bei Konzernen hat die Regelung zur Folge, dass jedes zum Konzern gehörige Unternehmen mit eigenständiger Rechtspersönlichkeit ein Verzeichnis führen muss.

2 c bb) Wer muss im Unternehmen das Verfahrensverzeichnis führen?

Dem betrieblichen Datenschutzbeauftragten kommt gemäß § 4 g 2 S. 2 die Aufgabe zu, die ihm im Unternehmen gelieferten Informationen (§ 4 e S. 1 Nr. 1 -8 BDSG) jedermann in geeigneter Weise verfügbar zu machen, das Verfahrensverzeichnis wird also beim **betrieblichen Datenschutzbeauftragten** geführt. Die Aufgabe zur Führung der Verzeichnisse (die häufig auch in der Bestellung zum DSB festgelegt ist) ändert aber nichts daran, dass das Unternehmen als verantwortliche Stelle die erforderlichen Informationen für das Verzeichnis **liefern muss** und auch formal verantwortlich bleibt.

Mit dem neu eingefügten **§ 4 g Abs. 2a** BDSG fällt diese Aufgabe dem **Leiter der verantwortlichen Stelle** zu, wenn keine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten besteht.

2 c cc) Auftragsdatenverarbeitung und Funktionsübertragung

Wenn ein Unternehmen einzelne Datenverarbeitungsprozesse oder auch seine gesamte Datenverarbeitung auf einen Dienstleister überträgt (z. B. im Rahmen von **Outsourcing**), ist für die Frage, wer die Verzeichnisse führen muss, zu unterscheiden. Liegt eine **Auftragsdatenverarbeitung** vor, so ist nicht der Dienstleister für die Einhaltung der gesetzlichen Daten-

schutzvorschriften verantwortlich, diese Verantwortlichkeit verbleibt vielmehr beim Auftraggeber, § 11 BDSG. Dementsprechend bleibt das abgebende Unternehmen die verantwortliche Stelle im Sinne des BDSG und hat daher auch alle Verzeichnisse (Verfahrensverzeichnis und Verarbeitungsübersicht) zu führen. Anders liegt es bei einer sog. **Funktionsübertragung**. Liegt eine solche vor, geht die Pflicht zur Führung der Verzeichnisse im Umfang der Übertragung auf den Dienstleister über (vgl. dazu auch unten 2 g). Die Abgrenzung zwischen einer Auftragsdatenverarbeitung und einer Funktionsübertragung kann im Einzelfall schwierig sein. Abgrenzungskriterien und nähere Erläuterungen dazu finden sich in den Begleitenden Hinweisen zur **BITKOM - Publikation „Mustervertragsanlage zur Auftragsdatenverarbeitung“**

Die BITKOM-Mustervertragsanlage zur Auftragsdatenverarbeitung kann unter dem folgenden Link abgerufen werden: http://www.bitkom.org/de/publikationen/1357_25976.aspx

2 d) Inhalt und Form des Verfahrensverzeichnisses

Entsprechend der Zielsetzung des öffentlichen Verfahrensverzeichnisses konzentriert sich der Inhalt des Verfahrensverzeichnisses auf die Offenlegung der für die Verarbeitung personenbezogener Daten verantwortlichen Stellen und Personen, auf die Zweckbestimmung der Verarbeitung, die betroffenen Personengruppen sowie die Nutzer und Empfänger der Daten und die Regelfristen für die Datenlöschung. Die inhaltliche Definition ist durch § 4 e BDSG, auf den in § 4 g Abs. 2 BDSG verwiesen wird, gegeben.

Da es sich bei den gesetzlichen Vorgaben eher um **Mindestanforderungen** handelt, dient das Verzeichnis interessierten Dritten lediglich als **Überblick** über die Verarbeitungsstrukturen personenbezogener Daten in Unternehmen und der öffentlichen Verwaltung. Rückschlüsse auf einzelne Verarbeitungsprozesse sind hierbei in der Regel nicht ableitbar und im Sinne der Zielsetzung auch nicht erforderlich. Es werden die Verfahren zwar einzeln benannt, jedoch hinsichtlich der Verarbeitungsmethoden summarisch beschrieben, d.h. einzelne Verfahrensschritte sind nicht zu melden. Bei tiefer gehenden Fragestellungen im Rahmen der Eigenkontrolle oder als Prüfbasis für Aufsichtsbehörden dienen dann die mehr detaillierten Verarbeitungsübersichten (vgl. 2 f,g), aus denen ggfs. (vgl. 2 b) die Angaben im Verfahrensverzeichnis abgeleitet sind.

Ein **Beispiel** für ein Verfahrensverzeichnis ist im Anhang als **Anlage 3** abgebildet.

Die **Art und Weise der Veröffentlichung** des Verfahrensverzeichnisses kann von der verantwortlichen Stelle selbst bestimmt werden. Selbst eine mündliche Auskunft ist rechtlich nicht ausgeschlossen. Die Veröffentlichung im Internet ist ebenso praktikabel wie die auf Antrag gezielte Weitergabe der Informationen in Form eines Formulars, das entsprechend der Aufzählung in § 4 e BDSG wie folgt gegliedert sein könnte:

Eine Auskunft in der von der verantwortlichen Stelle gewählten Form ist kostenfrei. Wünscht der Antragsteller hingegen die Auskunft in einer von dieser Form abweichenden Art und Weise, kommt eine Kostenbeteiligung des Antragstellers in Betracht.

- Name oder Firma der verantwortlichen Stelle
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Unternehmensverfassung berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen
- Anschrift der verantwortlichen Stelle
- Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung

- Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

- Empfänger oder Kategorien von Nutzern und Empfängern, denen die Daten mitgeteilt werden können

- Regelfristen für die Löschung der Daten

  - Welches Löschkonzept ist vorgesehen?
  - Wann werden welche Daten gelöscht?

- eine geplante Datenübermittlung in Drittstaaten

  - Angaben darüber, ob eine Datenübermittlung an Dritte stattfindet
  - Angaben darüber, ob eine Datenübermittlung an Dritte im Inland stattfindet
  - Angaben darüber, ob eine Datenübermittlung innerhalb der EU / EWR stattfindet
  - Angaben darüber, ob bei einer Übertragung an Dritte außerhalb der EU / EWR auf ein angemessenes Datenschutzniveau beim Empfängerland geachtet wird

Ein **Beispiel** ist im Anhang als **Anlage 3** beigefügt.

Beispiele für zur Zeit erhältliche Tools sind in Teil 4 dargestellt.

2 e) Wer trägt im Unternehmen die Verantwortung für die Verarbeitungsübersicht?

Die Aufgabe, eine Übersicht über die (eigentlich) meldepflichtigen Inhalte sowie über zugriffsberechtigte Personen dem betrieblichen Datenschutzbeauftragten zur Verfügung zustellen, kommt der verantwortlichen Stelle zu (§ 4 g Abs. 2 S.1 BDSG). Der betriebliche Datenschutzbeauftragte nimmt diese Informationen entgegen und hat die Funktion, die erhaltenen Informationen zu koordinieren und verfügbar zu machen sowie seine datenschutzrechtliche Prüfung darauf aufzubauen.

2 f) Form der Verarbeitungsübersicht

Weder in der EU-Richtlinie noch im BDSG gibt es Vorschriften darüber, in welcher Form die Verfahrensübersicht anzulegen ist. Eine der Aufgaben des betrieblichen Datenschutzbeauftragten ist es daher, sich seine eigenen Arbeitsunterlagen dafür zu erstellen. Ob dies in Papierform, mit Hilfe von kleinen, selbst erstellten Softwareprogrammen oder auch mit am Markt angebotenen Tools erfolgt, liegt im Ermessen des Datenschutzbeauftragten.

Während die Struktur des Verfahrensverzeichnisses durch die Gesetzesvorgaben in der Praxis weitgehend standardisiert worden ist, **unterscheiden** sich die Verarbeitungsübersichten der Fachbereiche untereinander hinsichtlich Aufbau, Detaillierung und Aussagefähigkeit stark oder sie fehlen sogar gänzlich – eine Folge der erheblichen Unsicherheit bzw. Unkenntnis. Dem betrieblichen Datenschutzbeauftragten kommt hier die wichtige Aufgabe zu, den Fachbereichen verständliche Erklärungen und Definition für die einzelnen, auszufüllenden Felder sowie möglichst auch praktische Beispiele zur Verfügung zu stellen.

Da keine bestimmte Form vorgegeben ist, kommen neben der Umsetzung als Formular auch die Realisierung durch Excel-Tabellen, als Access-Datenbank oder im html-Format ebenso in Betracht wie die Umsetzung durch den Einsatz von Softwareprogrammen.

Die folgenden Ausführungen beziehen sich nicht nur auf eine Verarbeitungsübersicht in Formularform, sondern haben Gültigkeit für **alle** aufgeführten Umsetzungsformen.

2 g) Inhalte der Verarbeitungsübersicht

Während die zur Erfüllung der Meldepflicht anzugebenden Daten zur Verantwortungsstruktur für die Verarbeitung personenbezogener Daten gemäß § 4 e BDSG lediglich in einem Hauptblatt geführt werden, empfiehlt es sich, alle weiteren gesetzlich definierten Informationen pro Einzelverfahren zu dokumentieren. Zusätzlich sind jeweils Angaben zur Datenherkunft, zur Rechtsgrundlage der Verarbeitung, zu Berechtigungskonzepten und zu den getroffenen Datenschutzmaßnahmen im Sinn des BDSG § 9 sowie der dazu gehörigen Anlage erforderlich, um das Datenschutzniveau der einzelnen Verfahren beurteilen zu können.

Die folgenden technischen und organisatorischen Datenschutzmaßnahmen sind als Mindestanforderungen im BDSG bereits festgelegt:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Zwecktrennungsgebot

Der **Detaillierungsgrad** der Verarbeitungsübersicht ist gesetzlich nicht vorgegeben. Maßgeblich für die Frage, wie detailliert die Angaben zu machen sind, ist daher der gesetzliche Zweck der Verarbeitungsübersicht. Die Verarbeitungsübersicht sollte diejenigen Einzelheiten enthalten, die für die gesetzlich vorgesehenen und betrieblich notwendigen Analysen und Auswertungen sowie für die Prüf- und Kontrolltätigkeiten erforderlich sind.

Sinnvoll kann es sein, sich an die in den unten dargestellten Softwareprogrammen vorgegebene Struktur anzulehnen. Individuelle Ergänzungen sind auch hier meist weiterhin möglich.

In Abhängigkeit der Unternehmensgröße und damit der Komplexität einzelner Verfahren kann es sogar notwendig sein, Einzelanwendungen innerhalb der Verfahren gesondert im oben genannten Sinn zu dokumentieren und zu bewerten. In der Verarbeitungsübersicht werden dann allerdings diese Anwendungen wieder im Kontext des Gesamtverfahrens dargestellt. **Insofern empfiehlt sich bei größeren Unternehmen die Verfahrens-Dokumentation in** drei Ebenen **zu gestalten:**

- das von den Fachstellen zu liefernde Anwendungsregister,
- die durch Bündelung von Anwendungen zu Verarbeitungsblöcken entstehende Verarbeitungsübersicht und
- das für die Information Dritter grob zusammengefasste Verfahrensverzeichnis.

Dementsprechend erhält der Datenschutzbeauftragte in der Praxis die meldepflichtigen Informationen sowie Angaben über zugriffsberechtigte Personen in Verantwortung der Geschäftsführung (vgl. § 4 g Abs. 2 Satz 1 BDSG, dazu 2 c bb) von den jeweils zuständigen Fachbereichen und entwickelt daraus die für die Datenschutzkontrolle notwendige Dokumentation.

Im Fall von **Outsourcing** im Sinne des § 11 BDSG „Auftragsdatenverarbeitung“ gibt es keine direkten Auswirkungen auf die Gestaltung der Verarbeitungsübersicht, da dies keine Auswirkungen auf die Verantwortlichkeit der „Verfahrens-Eigner“ und die Darstellungsstruktur hat. Lediglich der Hinweis auf den Umfang des Outsourcing sollte Bestandteil der Dokumentation sein. Auch die Einbeziehung externer Dienstleister führt nicht zu Änderungen der Übersicht, sondern wird nur als Merkmal festgehalten und im Rahmen der Berechtigungsvergabe berücksichtigt.

Sofern die Verarbeitung durch Outsourcing-Partner oder Dienstleister in einer vom Standort des verantwortlichen Unternehmens entfernten Region stattfindet, ist bei einer Prüfung der technischen und organisatorischen Maßnahmen durch die Aufsichtsbehörde ggfs. die Inanspruchnahme der Amtshilfe einer anderen Behörde erforderlich.

Im Fall einer **Funktionsübertragung** innerhalb oder außerhalb der EU geht die Verantwortung für das Verfahren wie auch die Verpflichtung zur Führung eines Verfahrensverzeichnisses bzw. einer Verarbeitungsübersicht auf den Vertragspartner über (vgl. schon oben 2 c cc). Hier ist lediglich die Daten-Übermittlung aus einer Vorverarbeitung in der Verarbeitungsübersicht festzuhalten.

Teil 3) Wie kann eine Verarbeitungsübersicht erstellt werden?

Bringschuld der Unternehmensleitung bzw. –mitarbeiter
Die Geschäftsführung des Unternehmens ist gesetzlich verpflichtet, den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Dazu gehört insbesondere, ihm die Übersichten der im Unternehmen verwendeten Datenverarbeitungsprogramme zur Verfügung zu stellen. Bei der Erstellung der Verarbeitungsübersicht hat das zur Folge, dass dem Datenschutzbeauftragten alle erforderlichen Informationen und Daten zu liefern sind (vgl. auch unten 3 c cc).

3 a) Verknüpfung der Erstellung mit anderen unternehmensinternen Organisations- und Erfassungsprozessen

Die Erstellung der Verarbeitungsübersicht kann eine sehr komplexe und umfassende Aufgabe sein, die in hohem Maße Zeit und Ressourcen bindet. Grundsätzlich sollte der betriebliche Datenschutzbeauftragte daher zuerst prüfen, ob es bereits ähnliche **Prozesse** im Unternehmen gibt, die mit der Erstellung und Pflege der Verarbeitungsübersicht **kombiniert** werden können. Dies sichert häufig die erforderliche unternehmensinterne Unterstützung. Eine Verknüpfung kann sich auch als hilfreich erweisen, um die notwendige regelmäßige Aktualisierung der Verarbeitungsübersicht durchzuführen.

Eine Anlehnung an folgende Prozesse kann sich beispielsweise anbieten:

- Einführung von Sicherheitsmanagement und –prozessen
- Erfassung von Geschäftsprozessen im Rahmen des Qualitätsmanagements
- Einbettung in interne Schutzbedarfsfeststellungen
- Absprache von internen Servicelevel-Agreements (SLA).
- zum Zusammenhang mit der gesetzlich vorgeschriebenen **Vorabkontrolle** (vgl. den Exkurs unten 3 b).

Dabei dürfen jedoch nicht die spezifischen datenschutzrechtlichen Anforderungen der Verarbeitungsübersicht aus den Augen verloren werden.

3 b) Frühzeitige Einbindung des Datenschutzbeauftragten

Damit die Ordnungsmäßigkeit der Verarbeitung personenbezogener Daten möglichst früh und dauerhaft gesichert werden kann, sollte der betriebliche Datenschutzbeauftragte schon **bei der Projektentwicklung** einbezogen werden und Projekte aktiv begleiten können. Denn zu den Aufgaben des betrieblichen Datenschutzbeauftragten gehört die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Der Datenschutzbeauftragte ist nach dem BDSG bereits **von Beginn an** über Vorhaben automatisierter Verarbeitungen von der verantwortlichen Stelle zu informieren (§ 4 g Abs. 1 Nr. 1 BDSG).

Darüber hinaus sollte der Datenschutzbeauftragte unbedingt **in alle Genehmigungsprozesse** für neue IT-Vorhaben **eingebunden** werden (z.B. als Mitglied der IT-Entscheidungsgremien, als Genehmigungsstufe in einem Antrags-Workflow etc.) um sicherzustellen, dass in der Zeit nach der ersten Abfrage die neuen Anwendungen nach gleichem Muster beschrieben werden.

Exkurs: Vorabkontrolle und Verarbeitungsübersicht

Eine Möglichkeit für den Datenschutzbeauftragten, sich in Genehmigungsprozesse einzubringen, stellt auch die Vorabkontrolle dar, die dann als Informationsquelle für die Erstellung der Verarbeitungsübersicht genutzt werden kann.

Die Vorabkontrolle gemäß § 4 d Abs. 5 BDSG dient der präventiven Untersuchung, ob durch die konkrete inhaltliche und organisatorische Ausgestaltung eines bestimmtes Datenverarbeitungsprojekts besondere Risiken für die Rechte und Freiheiten von Personen entstehen. Solche besonderen Risiken für die Rechte der Betroffenen können zum einen vorliegen, wenn es sich um die folgenden besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) handelt:

- Angaben über die rassische und ethnische Herkunft
- Politische Meinungen
- Religiöse oder philosophische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit
- Sexualleben
- Aufnahme von Gesundheitsdaten

Zum anderen können sich besondere Risiken ergeben, wenn die Verarbeitung der personenbezogenen Daten dazu geeignet ist, die Persönlichkeit des Betroffenen einschließlich seiner Fähigkeiten, seiner Leistungen oder seines Verhaltens zu bestimmen. Relevant kann das beispielsweise werden bei

- Bewertungen des Kaufverhaltens
- Leistungskontrollen
- Scoringverfahren
- Data-Mining

Die Vorabkontrolle ist nicht erforderlich, wenn

- zur Erhebung, Verarbeitung oder Nutzung eine gesetzliche Verpflichtung besteht,
- die Betroffenen ihre Einwilligung gegeben haben,
- die Zweckbestimmung aufgrund eines vertragsähnlichen Vertrauensverhältnisses oder eines Vertragsverhältnisses begründet ist,
- die automatisierte Datenverarbeitung keine besonderen Risiken enthalten.

Wird die Vorabkontrolle durchgeführt, können die eingehenden Informationen zugleich auch zur Erstellung der Verarbeitungsübersicht genutzt werden. Vorabkontrolle und Verarbeitungsübersicht sind auf diese Weise häufig eng miteinander verbunden.

Sind die oben beschriebenen Voraussetzungen gegeben, so ist die Vorabkontrolle auf jeden Fall durchzuführen. Dieses kann durch die Fachabteilung mit Hilfe einer vom Datenschutzbeauftragten entwickelten Checkliste durchgeführt werden. Es wird empfohlen, gemeinsam mit dem Datenschutzbeauftragten und dem Projektverantwortlichen die Checkliste zu erarbeiten.

Fortsetzung Exkurs Vorabkontrolle:

Zur inhaltlichen Prüfung sollten folgende Angabe gemacht werden:

- Erlaubnistatbestand der Datenverarbeitung
- Allgemeine Beschreibung des Projektes oder des Systems
- Wer ist die verantwortlichen Stelle
- Wer sind die Anwender und wer die Betroffenen (Mitarbeiter, Kunden, Lieferanten…)
- Auflistung der gespeicherten Daten (Art der Daten, Herkunft, schutzbedürftige/sensitive Daten, etc); ggf. Beifügung von Unterlagen über Datenmodelle, Musterauswertungen usw.
- Informationen zum Berechtigungskonzept (Zugriffsrechte)
- Gibt es Schnittstellen zu anderen Systemen?
- Werden Daten an Dritte übermittelt und falls ja, an wen?
- Erfolgt die Datenverarbeitung für das Projekt im Rahmen einer Auftragsverarbeitung?
- Sind die erforderlichen Maßnahmen für Rechte der Betroffenen vorgesehen?
- Welche Löschungsfristen sind geplant?
- Gibt es eine Planungen für eine Anwenderschulung?
- Welche Hard- und Software wird eingesetzt?
- welche technischen und organisatorischen Maßnahmen sind getroffen?
- Beurteilung der Vorabkontrolle mit Risikobewertung

Die Ergebnisse der datenschutzrechtlichen Prüfung sind vom Datenschutzbeauftragten zu dokumentieren.

Ende Exkurs Vorabkontrolle

3 c) Die Erstellung der Verarbeitungsübersicht

Zur besseren Verständlichkeit wird im Folgenden nicht die Erstellung in Verbindung mit einem weiteren Unternehmensprozess dargestellt (vgl. oben 3 a), sondern die **alleinige Erstellung einer Verarbeitungsübersicht.**

Die Erstellung der Verarbeitungsübersicht kann typischerweise in mehrere Phasen unterteilt werden:

3 c aa) Sensibilisierungsphase

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

Aktionen z.B.:

- Vorbereitung eines Mailings mit Hinweisen
- Ergänzend: Artikel für das Intranet
- Hinweis im Rahmen der allgemeinen Sensibilisierung der Mitarbeiter

3 c bb) Informationsphase

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

- die bestehenden Anwendungen mit personenbezogenen Daten
  als auch
- möglichst frühzeitig die geplanten neuen Projekte und Anwendungen

zu beschreiben sind. 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.

Aktionen z. B.:

- Erstellung von Übersichten und Erläuterungen, FAQs, Präsentation usw.
- Durchführung von Workshops
- Gemeinsame Bearbeitung eines Musterfalles

3 c cc) 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.

Mögliche **Verfahren/Verarbeitungen** zeigt Anlage 4 des Anhangs auf; ein **Beispiel für einen Fragebogen** gibt **Anlage 5.** Zweckmäßig kann es sein den Fragebogen so zu gestalten, dass seine Auswertung auch zur Bearbeitung weiteren Aufgaben, z.B. einem IT–Sicherheitskonzept beiträgt.

Zweckmäßig kann es sein, die automatisierten Verarbeitungen schon vorab definierten Verfahren zuzuordnen, auf die sich die Darstellung des Verfahrensverzeichnisses später beschränkt.

Es wird noch einmal darauf hingewiesen, dass als erster Prüfschritt die Frage zu beantworten ist, ob die in Frage kommende Verarbeitung personenbezogene oder personenbeziehbare Daten betrifft. Ist dies nicht der Fall, ist eine Fehlanzeige nach dem vorgegebenen Muster erforderlich.

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.

Aktionen z. B.:

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

3 c dd) Klärungsphase

Während der Bearbeitungszeit der Meldeformulare 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 Hotlinedienstes** eingerichtet werden. Nach Rückgabe der Meldungen schließt sich **eine inhaltliche**

Tipp: Klärung strittiger Punkte im direkten Dialog mit den Verantwortlichen der Fachbereiche.

Prüfung der Meldungen durch den betrieblichen Datenschutzbeauftragten an. 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.

Aktionen z. B.:
- Einrichtung eines temporären Hotlinedienstes
- Klärung offener Fragen bzw. Korrektur offensichtlich unklarer Angaben im Direktkontakt

3 c ee) Bearbeitungsphase

Die von den Fachbereichen vorgelegten einzelnen Verarbeitungs- bzw. Verfahrensübersichten sind vom Datenschutzbeauftragten zu **strukturieren**, d.h. sie müssen auf die einzelnen Aufgabenbereiche verdichtet werden, um auch für außen stehende Dritte Transparenz zu bieten. Praktisch bedeutet dies, dass alle Einzelübersichten in dem Verzeichnis des jeweiligen Aufgabenbereichs gesammelt werden und dieser Bereich dann Beschreibungsobjekt für die Verarbeitungsübersicht wird**.**

Ein **Beispiel** für eine mögliche Aufgliederung gibt **Anlage 4**.

Somit besteht die Möglichkeit, nach unterschiedlichen Detaillierungsgraden Auskünfte zu geben. Dabei bietet die Verarbeitungsübersicht einen groben Überblick über die Struktur der automatisierten Verfahren für die Öffentlichkeit. 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.

Aktionen z. B.:
- Umsetzung der Meldungen in die Verarbeitungsübersicht und das Verfahrensverzeichnis durch den betrieblichen Datenschutzbeauftragten
- Vorbereitung der Informations-/Präsentationsmethode

3 c ff) Pflegephase

Die Aktualisierung der Verarbeitungsübersicht 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 Verarbeitungsübersichten zu kontrollieren. Wenn die Verarbeitungsübersicht nicht **laufend aktualisiert** wird (z.B. durch Einbindung in andere Prozesse), ist eine Aktualisierung in regelmäßigen Abständen zu empfehlen, z. B. einmal jährlich.

Wichtig: Einbindung des Datenschutzbeauftragten in die relevanten IT- bzw. Geschäftsprozesse.

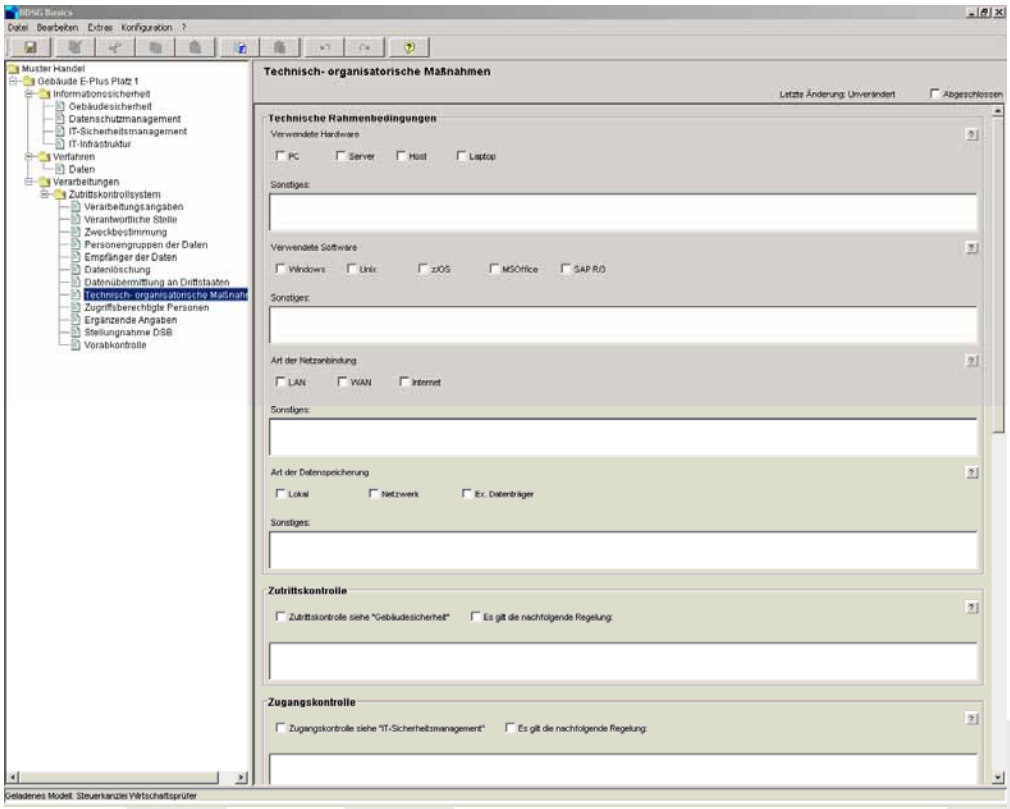
Aktionen z. B.:
- Aktualisierung der Dokumentation im Rahmen der Vorabkontrolle
- Überprüfung der Aktualität von Meldungen der Fachstellen durch die Kontrollfunktionen betrieblichen Datenschutzbeauftragten oder interne Revision

Teil 4) Beispiele für Programmtools für die Erstellung des Verfahrensverzeichnisses

Teil 4 stellt **keine abschließende Aufzählung** aller am Markt verfügbaren Softwaretools dar, sondern beschreibt lediglich einige **Beispiele**, mit denen das Autorenteam und die Mitglieder des BITKOM Arbeitskreises Datenschutz Erfahrungen sammeln konnten. Von der Darstellung anderer Softwaretools, zu denen noch keine eigenen Erfahrungen vorliegen, wurde abgesehen. In den jeweiligen Beschreibungen wurde zugunsten einer objektiven **Auflistung der Funktionalitäten** bewusst auf wertende Elemente verzichtet. Die Darstellung beschränkt sich auf die im Text angegebene Version, zu etwaigen Folgeversionen können in diesem Rahmen keine Ausführungen gemacht werden.

4 a) „BDSG Basics“ (Version 1.05.0)

Anbieter: Demal GmbH



Die Software wurde laut Anbieter mit Unterstützung der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) sowie der bayerischen Aufsichtsbehörde für den nicht öffentlichen Dienst und verschiedenen Datenschutzbeauftragten der freien Wirtschaft erstellt.

Das Programm wird in zwei Varianten angeboten: „BDSG Basics“ und „BDSG Basics Expert“. Die in den Werbeunterlagen besonders hervorgehobenen Funktionen der Basisversion sind: Vorgefertigte Datenschutz-Vorlagen für verschiedene Bereiche (bei denen bestimmte Vorgaben schon enthalten sind), eine „umfangreiche Programm-Hilfe in verständlichem Deutsch“, Musterformulare und Gesetzestexte, Export als PDF-Datei und eine „sichere“ Verschlüsselung (Passwortschutz).

Die **BDSG Basics Expert Version** soll zusätzlich folgende Funktionen enthalten: Mandantenfähigkeit, Netzwerkfähigkeit, Exportmöglichkeit in RTF-Format, unterschiedliche Layouts für Mandanten, Datensicherungsmöglichkeiten, Verarbeitungen mit Planungsstatus und

mehr Eingabefelder für eine genauere Erfassung. Die Version BDSG Basics Expert richtet sich vom Funktionsumfang her im Wesentlichen an externe Datenschutzbeauftragte.

Die weiteren Darstellungen beziehen sich ausschließlich auf die **Basisversion**. Unternehmen können hier in Unternehmenseinheiten untergliedert werden, was z.B. dann sinnvoll sein kann, wenn getrennte Gebäude unterschiedliche Sicherheitsstandards aufweisen, die man dokumentieren möchte. Es bestehen vorgefertigte Unternehmensmodelle (z.B. Steuerkanzlei/Wirtschaftsprüfer, Handel, Industrie und Bank), die bereits in manchen Punkten (im Wesentlichen bei der Verfahrensübersicht) vorkonfiguriert sind.

Nach dem Start der Software sind drei Module sichtbar: „Informationssicherheit“, „Verfahren“ und „Verarbeitungen“.

Das Modul „**Informationssicherheit**“ enthält Unterrubriken zu den Themen Gebäudesicherheit, Datenschutzmanagement, IT-Sicherheitsmanagement und IT-Infrastruktur:

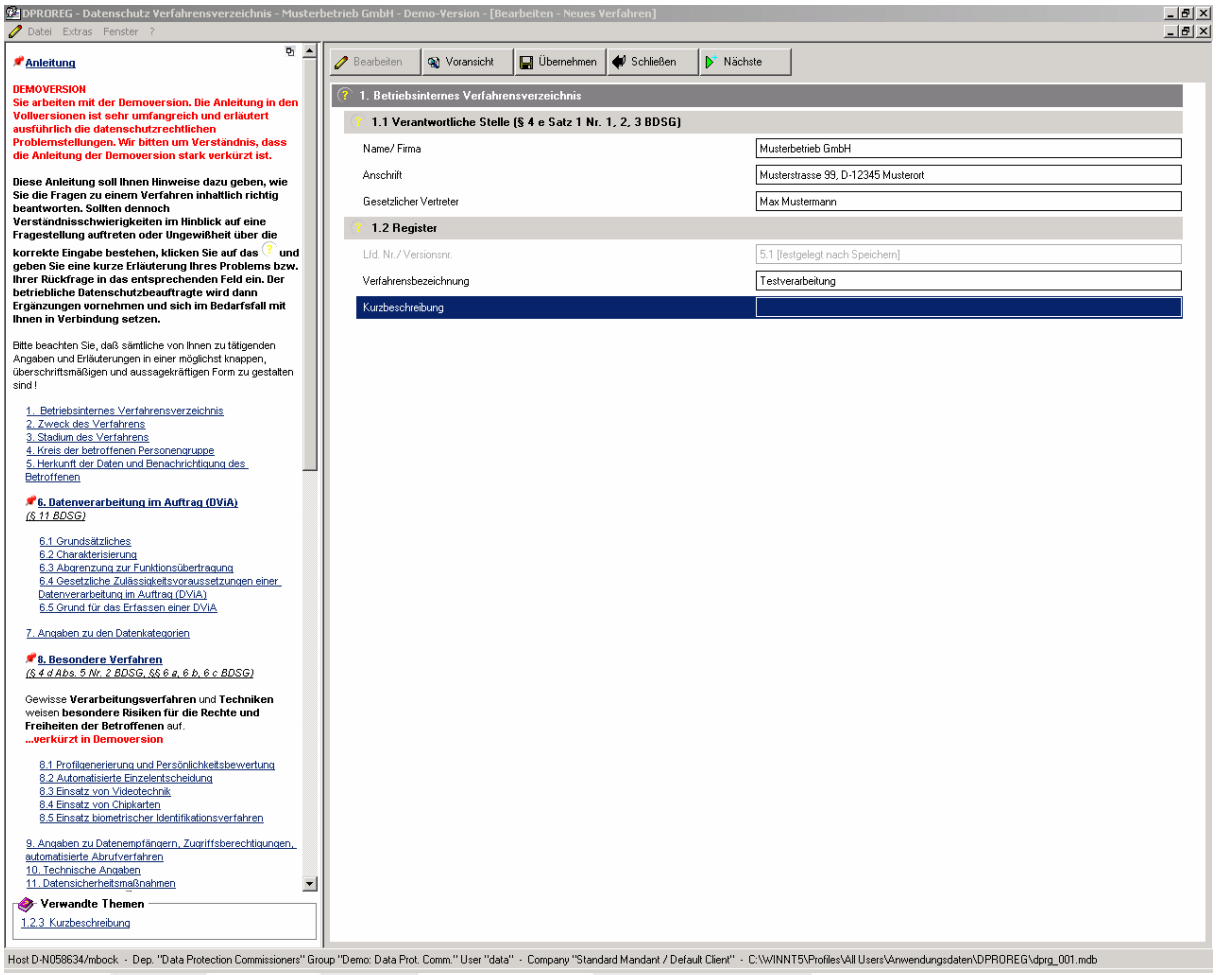
- Im Teil **Gebäudesicherheit** werden Informationen zur Zutrittskontrolle erfasst und eine Klassifizierung nach Sicherheitsbereichen vorgenommen.
- Im Teil **Datenschutzmanagement** werden Angaben zum Datenschutzbeauftragten und dessen Aufgaben sowie zum Tätigkeitsumfeld als auch zur innerbetrieblichen Organisation gemacht.
- Die Rubrik **IT-Sicherheitsmanagement** beinhaltet weitere Sicherheitsmaßnahmen wie Zugangs- und Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle und Verfügbarkeitskontrolle.
- Die Rubrik **IT-Infrastruktur** dient zum Einfügen weiterer Dokumente.

Die beiden weiteren Module beschäftigen sich mit dem eigentlichen Verfahrensverzeichnis und der internen Verfahrensübersicht. Unter „Verfahren“ können die Angaben für das (öffentliche) Verfahrensverzeichnis gemacht werden, die Fragen halten sich an die Reihenfolge des § 4 e BDSG. Unter „Verarbeitungen“ werden die Angaben für die interne Verarbeitungsübersicht erfasst. Im Rahmen der Erfassung der Verarbeitungen kann teilweise auf Eingaben in den Teilen IT-Sicherheitsmanagement und Gebäudesicherheit verwiesen werden oder es können die Regelungen zu den technisch-organisatorischen Maßnahmen (vgl. Anlage zu § 9 BDSG) neu eingegeben werden. Abschließend gibt es noch die Eingabemasken „Stellungnahme des DSB“ sowie „Vorabkontrolle“. Inklusive der Vorabkontrolle sind pro Verarbeitung 12 Fragenkomplexe zu absolvieren.

Die Software enthält eine umfangreiche Programmhilfe, die auch weiterführende PDF-Dokumente, ein Glossar, Datenschutz-Adressen und Internet-Links enthält.
Es ist möglich, bereits erfasste Inhalte in andere Verarbeitungen zu übernehmen. Eine Funktionen zur „automatischen Generierung" des Verfahrensverzeichnisses war nicht vorhanden; von einer solchen Funktion darf man sich aber auch keine große Erleichterung versprechen.

4 b) „DPROREG Verfahrensverzeichnis“ (Version 2.1)

Anbieter: Software Objects GmbH



Von der Software DPROREG sind verschiedene Versionen erhältlich: Start-Edition, Single-User-Edition, Multi-User-Edition sowie eine Demoversion. Die DPROREG Start-Edition ist eine Einzelplatzversion, mit der ein User einen Mandanten verwalten kann. Sie ist gedacht für betriebliche DSB in kleinen mittelständischen Unternehmen. Sie bietet fünf vordefinierte Auswertungen, vorhandene Systemauswertungen sind nicht editierbar. Es besteht die Möglichkeit Fragen frei zu editieren, um die Anwendung an unternehmensspezifische Gegebenheiten anzupassen.

Die DPROREG Single-User-Edition ist insbesondere für externe Datenschutzbeauftragte und größere mittelständische Unternehmen geeignet, es handelt sich zwar ebenfalls um eine Einzelplatzversion, es bestehen aber keine Einschränkungen bezüglich der Anzahl der Mandanten und der Anzahl der kritischen Auswertungen. Die Auswertungen sind frei definierbar. Die Systemauswertungen für „kritische Verfahren“ sind editierbar. Die Version ist im Gegensatz zur Start Edition zweisprachig (Deutsch/Englisch).
Darüber hinaus bietet die Software Objects GmbH eine „DPROREG Multi-User-Edition“ an, die neben frei definierbaren Benutzerrollen auch die Möglichkeit beinhaltet, eine unbegrenzte Anzahl von Clients und User zu verwalten. Weiterhin wird zur Zeit gerade an einer **Enterprise-Edition** gearbeitet.

Zu Beginn der Arbeit sieht man auf der linke Seite ein großzügiges Hilfefenster, was den Einstieg in das Programm und die weitere Bearbeitung deutlich erleichtert. Hilfe zu den einzelnen Fragen ist kontextbezogen verfügbar. Die Anleitung in der Vollversion soll nach den

Angaben des Anbieters sehr umfangreich sein und ausführlich die datenschutzrechtlichen Problemstellungen erläutern. Bereits in der Demoversion erhält man einen ersten Eindruck davon. Von der grafischen Gestaltung ist das Programm sehr ansprechend programmiert, insbesondere wurde Wert auf hohe Kontrastfähigkeit gelegt. Bei der Eingabe sind alle Fragen zu beantworten bzw. durchzuklicken. Es besteht für den Ausfüllenden die Möglichkeit, zu den einzelnen Rubriken und Fragen Rückfragen zu hinterlegen, zu denen der betriebliche Datenschutzbeauftragte dann ggf. Rücksprachen halten kann oder weitere Ergänzungen machen kann. Bezüglich technischer organisatorischer Maßnahmen kann zwischen Grundschutz und hoher Sicherheitsbedarf unterschieden werden. Unter „Programm Optionen“ können Vorbelegungen für die verantwortliche Stelle etc. hinterlegt werden, so dass diese bei der nächsten Erfassung übernommen werden.

In der Gesamtübersicht gibt es verschiedene Spalten, in denen der Status der Verfahren graphisch angezeigt wird. Es gibt die Spalte „DSB Status“, wo z.B. vermerkt wird, ob der DSB das Verfahren geprüft hat. Aus der Spalte „Verfahrensstatus“ lässt sich hingegen ablesen, ob z.B. das Verfahren komplett ausgefüllt worden ist. Per Button kann man sich durch die offenen Punkte einer Verarbeitungsübersicht klicken, dabei werden auch alle optionalen Fragen der Reihe nach angesteuert.

4 c) „DSBbrain 2000“ (Version 1.3.5)

Anbieter: Black Brain Medien Dienste, Entwicklungsbüro Ulf Hillig

Eine Demoversion der Software DSB*brain* ist nicht verfügbar, die folgenden Angaben beziehen sich daher aus den im Internet verfügbaren Produktinformationen. Eine Nachfolgeversion 2.x ist derzeit in Vorbereitung. Eine öffentliche Beta-Version wurde im November 2005 angekündigt.

DSB*brain* 2000 ist **keine reine Verfahrensverzeichnislösung**, sondern versteht sich als „Arbeits- und Informationssystem zur Unterstützung organisatorischer und gesetzlicher Aufgaben des betrieblichen und behördlichen Datenschutzbeauftragten inklusive Rechts- und Literaturarchiv“ und soll helfen, die tägliche Arbeit des Datenschutzbeauftragten zu organisieren, notwendige Informationen zu gewinnen und zeitnah die geforderten Nachweise, Register und Dokumentationen zu führen. So besteht die Möglichkeit Anfragen von Betroffenen zu dokumentieren; Informationen über besuchte Seminare, Tagungen und Workshops können unter dem Modul Fachkunde gespeichert werden. Darüber hinaus können im Modul Schulungen Mitarbeiterschulungen dokumentiert werden. Eine Adressdatenbank enthält Anschriften und „virtuelle“ Kontaktmöglichkeiten von Aufsichtsbehörden, Ministerien, Gerichten usw. Eine integrierte Textverarbeitung und vorbereitete Mustertexte sind ebenfalls enthalten. In die Software integriert sind eine Gesetzessammlung und zahlreiche Artikel und Literaturan-

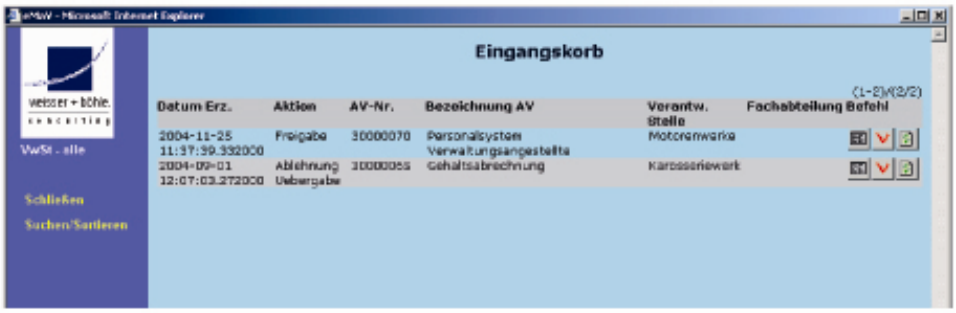
gaben. Die Software ist mandantenfähig und bietet die Möglichkeit, Verarbeitungs- und Nutzerregister zu führen. Das Verarbeitungsregister erfasst alle automatisierten Verarbeitungen des Unternehmens. Unterschiedliche technische und organisatorische Maßnahmen werden länderspezifisch zugewiesen. Auf Knopfdruck erfolgt die automatische Ausgabe des Verfahrensverzeichnisses. In dem Nutzerregister wird einzeln oder gruppenweise die Teilnahme an Schulungen. Verpflichtungen sowie Zugriffe auf automatisierte Dateien ausgewiesen.

Zu der Software werden auch ca. 1,5 Tage dauernde Trainingsveranstaltungen angeboten. Der Mehrwert schlägt sich im ungefähr doppelt so hohen Preis der Software gegenüber reinen Lösungen für das Verfahrensverzeichnis nieder.

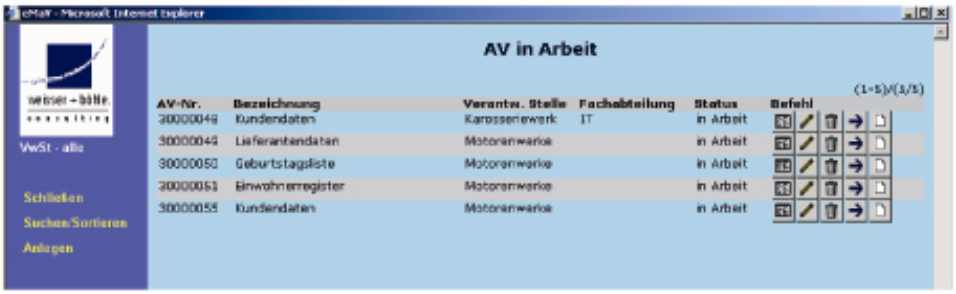
4 e) „EMaVLight“

Anbieter: Weisser + Böhle GmbH

Eingangskorb (automatisch bei Programmstart):



Listensicht automatisierte Verarbeitungen:



EMaV steht für „elektronisches Melderegister für automatisierte Verarbeitungen“. Eine Demoversion steht für die Software nicht zur Verfügung, es besteht aber die Möglichkeit einer (kostenpflichtigen) Testinstallation. Die Angaben im Folgenden beziehen sich daher auf die **Angaben des Herstellers** und konnte nicht überprüft werden.

Die Software richtet sich an größere Unternehmen und Behörden und will Bearbeitungsprozesse im Unternehmen durch einen integrierten Workflow unterstützen. Die Software erleichtert dem Datenschutzbeauftragten das Führen eines Melderegisters nach § 4 g BDSG und ermöglicht gleichzeitig der verantwortlichen Stelle die Bereitstellung der benötigten Informationen. Zusätzlich können Daten im Zusammenhang mit automatisierten Verarbeitungen verarbeitet werden sowie technisch und organisatorische Maßnahmen zum Datenschutz, so dass eMaV alle Anforderungen an eine Verarbeitungsübersicht erfüllen soll. EMaV bietet Möglichkeiten die Verarbeitungsübersicht elektronisch zu erstellen, zu pflegen und auszuwerten. Durch einen integrierten Workflow soll die Zusammenarbeit zwischen dem Datenschutzbeauftragten und den Vertretern der verantwortlichen Stelle unterstützt werden.

Die Software bietet sowohl vorgefertigte Auswertungen als auch die Möglichkeit individueller Konfiguration. EMaV basiert auf einem Java-Applikationsserver und einer relationalen Datenbank. Der Nutzer benötigt für den Aufruf der Applikation einen Internet Browser. Auswertungsmöglichkeiten und ein Rollenkonzept sind vorhanden

Mit eMaVLight erhält man eine Einsteiger-Lizenz, mit der bis zu fünf Nutzer verwaltet werden können. Für mehrere verantwortliche Stellen benötigt man ein oder mehrere UserPacks oder OrgPacks. Für große Betriebe und Organisationen ist eMaV Enterprise gedacht.

	Anbieter	Demo-version	Export-funktionen	Vorab-kontrolle	Passwort-schutz	Netzwerkfähigkeit	Auswertungs-möglichkeiten	Mandantenfähigkeit, Eignung für externe DSB
BDSG Basic Version 1.05.0	Demal GmbH, Hembacherstr. 2b, 90592 Schwarzenbruck, E-Mail info@demal-gmbh.de, www.demal-gmbh.de	Ja	Ja (als PDF)	Integriert	Ja	Ab BDSG Basics Expert	Nein	Nur in der BDSG Basic Expert Variante
DPROREG Verfahrensverzeichnis Version 2.1	Software Objects GmbH, An der Steinernen Bank 1, 93080 Pentling, info@dproreg.com, www.dproreg.com	Ja	Ja (als html-Dokument))	Integriert	Ja.	Ab DPROREG Multi-User version	Ja	Ab DPROREG Single User Edition
DSB*brain* 2000 Version 1.3.5	Black Brain Medien Dienste Entwicklungsbüro Ulf Hillig Am Ziegelgrund 28 01744 Dippoldiswalde	Nein	Über Druckfunktion Ausgabe in RTF-Format*	Integriert*	Ja*		Suchmöglichkeiten bestehen*	Mandantenfähig unlimitiert*
eMaVLight	Weisser + böhle GmbH Schwieberdinger Str. 52 71636 Ludwigsburg info@weisserboehle.de, www.weisserboehle.de	Nein	---	---	Ja+ Rollenkonzept*	Ja*	Ja*	Nein

* laut Herstellerangaben

Teil 5) Anhang

Der Anhang enthält die folgenden **Anlagen zu den Teilen 2 und 3** der Publikation:

- Anlage Nr. 1: Welche Unternehmen sind verpflichtet, einen Datenschutz-beauftragten zu bestellen?
- Anlage Nr. 2 Übersichtstabelle neu
- Anlage Nr. 3: Beispiel für ein Verfahrensverzeichnis
- Anlage Nr. 4: Einzelne mögliche Verfahren, die in der Verarbeitungs-übersicht erfasst sind
- Anlage Nr. 5: Formulare zur Verarbeitungsübersicht
- Anlage Nr. 6: Erläuterungen zu den Inhalten der Formulare in Anlage 4

Anlage 1: Verpflichtung einen Datenschutzbeauftragten zu bestellen

Welche Unternehmen sind verpflichtet, einen Beauftragten für den Datenschutz zu bestellen?

Die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten im nicht-öffentlichen Bereich besteht,

a) wenn personenbezogene Daten automatisiert verarbeitet werden und mindestens neun Personen mit der automatisierten Verarbeitung personenbezogener Daten ständig beschäftigt sind, § 4 f Abs. 1 S. 1, 4 BDSG (Beispiele: Versicherungen, Kreditinstitute, Handelsfirmen, Handwerksbetriebe)

oder

b) wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind, § 4 f Abs. 1 S. 3 BDSG (diese Alternative dürfte heute allerdings nur noch geringe praktische Relevanz haben).

Diese Mindestvoraussetzungen entfallen allerdings, wenn sich aus der Art der verarbeitenden Daten bzw. der Verwendungszwecke besondere Gefährdungen oder Risiken für das Persönlichkeitsrecht der Betroffenen ergeben können. Das betrifft Unternehmen,

a) wenn eine Vorabkontrolle durch den Datenschutzbeauftragten gem. § 4 d Abs. 5 erforderlich ist (§ 4 f Abs. 1 Satz 6 1. Alternative, Beispiel: Dienstleister im Gesundheitswesen), zur Vorabkontrolle vgl. oben den Exkurs in 3 b.

oder

b) wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymen Übermittlung erhoben, verarbeitet oder genutzt werden (§ 4 f Abs. 1 Satz 6 2. Alternative, Beispiele: Auskunfteien, Markt- und Medienforschungsinstitute).

Ist ein Unternehmen nach einer dieser Vorschriften zur Bestellung eines Beauftragten für den Datenschutz verpflichtet, so muss es diese Verpflichtung spätestens innerhalb eines Monats erfüllen, nach dem es die Daten verarbeitende Tätigkeit aufgenommen hat.

Durch das „Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere der mittelständischen Wirtschaft“ vom 26.08.2006 wird nunmehr ausdrücklich klargestellt, dass auch **Amts- und Berufsgeheimnisträger** wie Ärzte und Rechtsanwälte und Steuerberater einen **externen Datenschutzbeauftragten** bestellen können. Die Kontrollbefugnis des Beauftragten für den Datenschutz erstreckt sich nach § 4 f Abs. 2 nun auch auf personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Bisher war dies streitig, da ohne die Neuregelung bei einem Zugriff auf die oben genannten Daten eine unbefugte Offenbarung im Sinne des § 203 StGB hätte vorliegen können. Als weitere Folge der Neuregelung ist der Geheimnisverrat von „fremden Geheimnissen“ durch den DSB nun in § 203 Abs. 2a StGB auch für den DSB unter Strafe gestellt worden. In § 4f Abs. 4a BDSG ist darüber hinaus ein Zeugnisverweigerungsrecht für Informationen der Berufsgeheimnisträger, welche dem DSB zur Kenntnis kommen, auch für den DSB und seine Hilfspersonen einge-

führt worden. Im Gesundheitsbereich kann die Beschäftigung eines externen DSB aber immer noch daran scheitern, dass in einzelnen Bundesländern die Beschäftigung für bestimmte Bereiche ausgeschlossen ist. Z.B. dürfen in einigen Bundesländern keine externen DSB in staatlichen Krankenhäusern beschäftigt werden.

Anlage 2: Übersicht zu Meldepflicht, Bestellung, Verfahrensverzeichnis und Verarbeitungsübersicht

Liegt die Meldepflicht vor?	**Ist die Bestellung eines betr. DSB erforderlich?**	**Ist ein Verfahrensverzeichnis erforderlich?**	**Ist eine Verarbeitungsübersicht erforderlich?**
1. (+) bei Verfahren automatisierter Verarbeitung § 4 d 1 BDSG	1. Alt (+) wenn pbD automatisiert verarbeitet werden § 4 f 1 S.1 BDSG	(+) immer (! Klarstellung durch den neuen § 4 g **2 a** BDSG, der die Lücke schließt, die vorher uU bei Spalte 1, 3. Alt. -je nach Auslegung- vorgelegen hat) 1. Alt: Dem bDSB ist von der verantwortlichen Stelle eine Übersicht über die meldepflichtigen Angaben (§ 4 e S.1 BDSG) sowie die zugriffsberechtigten Personen zur Verfügung zu stellen § 4 g Abs. 2 S. 1 BDSG	(+) wenn ein bDSB bestellt worden ist Dem bDSB sind die erforderlichen Informationen von der verantwortlichen Stelle zur Verfügung zu stellen.
2. (-) bei Bestellung eines betrieblichen DSB § 4 d 2 BDSG	2. Alt (+) wenn pbD auf andere Weise erhoben, verarbeitet oder genutzt werden und mindestens 20 Personen damit beschäftigt sind § 4 f 1 S. 3 BDSG	2. Alt: Soweit keine Verpflichtung zur Bestellung eines DSB besteht (siehe 2. Spalte Ziffer 5), hat der Leiter der verantwortlichen Stelle die Erfüllung der Aufgaben nach § 4 g Abs. 2a S. 1 BDSG in anderer Weise sicherzustellen, d.h. er hat auch sicherzustellen, dass das Verfahrensverzeichnis jedermann in geeigneter Weise verfügbar ist.	Ob § 4 g 2a S.1 BDSG zur Folge hat, dass der Leiter der verantwortlichen Stelle auch eine Verarbeitungsübersicht führen muss, ist fraglich. Dem Gesetzeszusammenhang und der Begründung (des BRats) lässt sich das nicht mit Sicherheit entnehmen. Zu beachten ist, dass Verfahrensverzeichnis und Verarbeitungsübersicht selbständige Instrumente sind. In Relation zur Komplexität der

			Verarbeitung kann daher auf eine Verarbeitungsübersicht ggf. auch verzichtet werden.
3. (-) wenn neun oder weniger Personen mit Erhebung, Verarbeitung oder Nutzung beschäftigt sind und Einwilligung der Betroffenen vorliegt oder Vertrags-/Vertrauensverhältnis § 4 d 3 BDSG	3. (+) unabhängig von der Personenzahl: soweit die automatisierte Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen und daher eine Vorabkontrolle (§ 4 d 5 BDSG) vorgeschrieben ist § 4 f 1 S. 6 BDSG		
Die Meldepflicht entfällt bei 2. und 3. NICHT, wenn geschäftsmäßig pbD gespeichert werden zum Zwecke der Übermittlung oder zum Zwecke der anonymisierten Übermittlung. § 4 d 4 BDSG	4. (+) unabhängig von der Personenzahl: wenn geschäftsmäßig pbD gespeichert werden zum Zwecke der Übermittlung oder zum Zwecke der anonymisierten Übermittlung § 4 f 1 S. 6 BDSG		
	5. : Ausnahme (-) bei 1. Alt: wenn in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung von pbD beschäftigt sind § 4 f 1 4 BDSG		

Anlage 3: Beispiel Verfahrensverzeichnis

1. Name und Anschrift der verantwortlichen Stelle

Mustermann Marketing GmbH
Eckstr. 5, 60437 Frankfurt

Standort Offenbach
Senefelderstr. 160, 63069 Offenbach

2. Geschäftsleitung

Manfred Mann, Managing Director, Frankfurt

Hubert Kah, Managing Director, Offenbach

3. Leiter der Datenverarbeitung der verantwortlichen Stelle

Peter Kraus, Director, Frankfurt

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 Personengruppen

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 so-

wie 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 oder Kategorien von Empfängern der Daten

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. Datenübermittlung in Drittländer

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.

8. 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 Vertragserfüllung 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. abgelehnten Bewerbungen oder Abmahnungen). Sofern Daten hiervon nicht berührt sind, werden sie gelöscht, wenn die unter 5. genannten Zwecke wegfallen.

Mustermann Marketing GmbH
Datenschutzbeauftragter

Frankfurt, 25.01.2005

TIPP: Viele Unternehmen veröffentlichen ihre Verfahrensverzeichnisse im Internet, so dass **branchenspezifische Beispiele** leicht auffindbar sind.

Anlage 4: Verfahren

Einzelne/mögliche Verfahren, die in der Verarbeitungsübersicht erfasst sind:

Verfahren bezeichnen Kategorien automatisierter Verarbeitungen, wie sie auch im Verfahrensverzeichnis oft aufgeführt werden.

Die folgende Auflistung von Verfahren hat lediglich **Beispielscharakter** und erhebt keinen Anspruch auf Vollständigkeit. Sie sollten daher für das jeweilige Unternehmen geprüft und dann ggf. an die Strukturen und Prozesse des Unternehmens **angepasst bzw. entsprechend ergänzt** werden.

1. **Verfahren: Bürokommunikation/Office**

   Mögliche automatisierte Verarbeitungen
   Erstellung von Berichten und Auswertungen mit Standardwerkzeugen der Bürokommunikation.
   Erstellung, Steuerung, Archivierung von Informationen, Dokumenten und Geschäftsprozessen.

2. **Verfahren: Produkt-Vertrieb und Erbringung von Dienstleistungen**

   Mögliche automatisierte Verarbeitungen
   Verkauf oder Vermietung von Produkten, Erbringung von Dienstleistungen

   Dokumentation der für Kunden erstellten Angebote sowie der erteilten Kundenaufträge in Verbindung mit personenbezogenen Daten von Mietern, Käufern, Dienstleistungsempfängern.
   Verarbeitung von personenbezogenen Daten zur Auftragsabwicklung und Service-Bereitstellung.

3. **Verfahren: Verarbeitung von Daten über Nichtkunden/Kunden/Interessenten**

   Mögliche automatisierte Verarbeitungen
   Verwaltung personenbezogener Daten über Nichtkunden zwecks Akquisition
   Gewinnung und Verwaltung personenbezogener Daten von Kunden und Interessenten zu Marketingzwecken (CRM).

4. **Verfahren: Durchführung von Service-Aufträgen**

   Mögliche automatisierte Verarbeitungen
   Bearbeitung von Service-Aufträgen in Bezug auf die bei Kunden installierten Produkte. Speicherung personenbezogener Daten in Verbindung mit Produktdaten im Hinblick auf eine schnelle zielgerichtete Leistungserbringung.

5. Verfahren: Logistik/Versandsteuerung

Mögliche automatisierte Verarbeitungen
Kundenbezogene Zusammenstellung der auszuliefernden Produkte. Speicherung personenbezogener Daten zur Versandsteuerung.

6. Verfahren: Personaldatenverwaltung

Mögliche automatisierte Verarbeitungen
Berechnung und Zahlung von Löhnen, Gehältern, Betriebsrenten, Spesen, Provisionen und sonstigen vertraglichen oder sozialen Leistungen (sämtliche zur Ermittlung der Vergütung erforderlichen Informationen), die Verwaltung von Personaldaten zur Personalbetreuung (einschl. der Personalplanung/-entwicklung, Aus- und Weiterbildung), Informationen zur Gewährung gesetzlicher und freiwilliger Sozialleistungen, Organisation von Versetzungen, Beförderungen und Neueinstellungen (Bewerbern), Sicherstellung der Mitbestimmungsrechte durch die Mitarbeitervertretung

7. Verfahren: Verarbeitung von Daten von Lieferanten/Dienstleistern (z.B. Provider, Auftragsverarbeiter)

Mögliche automatisierte Verarbeitungen
Verwaltung personenbezogener Daten von regelmäßigen Leistungsanbietern wie Lieferanten, Beratern, Outsourcing-Partnern usw. zwecks Ausschreibung, Einkauf, Vertragsabwicklung und Betreuung.

8. Verfahren: Verarbeitung von Daten innerhalb von Entwicklungs- und Produktionsprozessen

Automatisierte Verarbeitung von personenbezogenen Daten im Rahmen von Entwicklung und Produktionsprozessen (z. B. Entwicklungsdokumentationen).

9. Verfahren: Betrieb von Datenverarbeitungs- und TK-Anlagen im Kundenauftrag

Mögliche automatisierte Verarbeitungen
Sicherstellung eines ordnungsmäßigen DV-/TK-Betriebes im Kundenauftrag (Outsourcing-Geschäft). Bereitstellen von Kontrollmechanismen, Log-Dateien, Protokollen, Berechtigungs-, Sicherheits- und Sicherungsverfahren.
(z.B. Benutzerdaten von MA, Administratoren, externe Mitarbeiter und Berechtigte)

10. Verfahren: Verarbeitung von personenbezogenen Daten im Rahmen der Hausverwaltung und Objektsicherung

Mögliche automatisierte Verarbeitungen
Wahrnehmung des Hausrechts, um z.B. den Zutritt Berechtigter zu regeln, den Publikumsverkehr in den öffentlich zugänglichen Bereichen zu überwachen sowie Wahrnehmung berechtigter Interessen wie Sammlung von Beweismitteln bei Vandalismus (z.B. Videoüberwachung).

Anlage 5: Formulare zur Verarbeitungsübersicht

Die folgenden Formulare

- Fehlanzeige
- Meldung einer automatisierten Verarbeitung
- Interner Prüfvermerk des Datenschutzbeauftragten

dienen der Datenerfassung für die Meldungen der Fachstellen, d.h. sie sind die Basis für die Gestaltung der Verarbeitungsübersicht und gleichzeitig auch Grundlage für das in Anlage 3 beispielhaft dargestellte Verfahrensverzeichnis.

Das Formular „Fehlanzeige“ dient zur Meldung an den Datenschutzbeauftragten, dass keine personenbezogene Daten in der jeweiligen automatisierten Verarbeitungen verarbeitet werden; für die jeweilige automatisierte Verarbeitung ist die „Meldung einer automatisierten Verarbeitung“ auszufüllen; der „Interne Prüfvermerk“ schließlich dient der Dokumentation der Tätigkeit des Datenschutzbeauftragten, hier können Angaben zu einer Vorabkontrolle oder Wiedervorlage aufgenommen werden.

Erläuternde Hinweise zu einzelnen Feldern sind als Anlage 5 aufgelistet.

Die Formulare haben lediglich **Beispielscharakter**. Sie sollten daher für das jeweilige Unternehmen geprüft und dann ggf. an die Strukturen und Prozesse des Unternehmens **angepasst bzw. entsprechend ergänzt** werden.

5.1 Formular „Fehlanzeige“

In einem ersten Prüfschritt ist festzustellen, ob eine Verarbeitung/Anwendung personenbezogene Daten enthält. Ist das nicht der Fall, so ist diese Meldung mittels des folgenden Formulars abzugeben. Damit wird erreicht, dass alle Verfahren/Anwendungen im Unternehmen registriert und damit prüfbar sind.

Fehlanzeige zur Meldung von automatisierten Verarbeitungen nach § 4e BDSG (bitte an den Datenschutzbeauftragten übersenden)				
Nur auszufüllen, wenn keine personenbezogenen Daten verarbeitet werden! Hinweis Nr. 1				
Projekt-Nr.: Hinweis Nr. 2	☐	**Änderung bestehendes Verfahren**	☐	**Eigenentwickelte Software**
ggf. Einführungstermin: Hinweis Nr. 3	☐	**neues Verfahren**	☐	**Standard- bzw. Kauf-Software**
1. Grundsätzliche Angaben zum Verfahren und zur Verantwortlichkeit.				
1.1	Bezeichnung und genaue Beschreibung des Verfahrens:			
1.2	Fachbereich:	Verantwortliche Führungskraft:	ggf.: Stellen-Kennzeichen:	
1.3	Ausfüllende Person:		Telefon-Nummer:	

Hiermit bestätigen wir, dass das oben näher bezeichnete Verfahren keine personenbezogene Daten Hinweis Nr. 1 **verarbeitet und deshalb nicht in das öffentliche Verfahrensverzeichnis aufgenommen werden muss.**

Uns ist bekannt, dass eine Änderung des Verfahrens, insbesondere dann wenn personenbezogene Daten verarbeitet werden, eine Meldung erforderlich machen.

Datum: *Unterschrift der Führungskraft:*

5.2 Formular „Meldung einer automatisierten Verarbeitung“

Für jedes einzelne betriebene automatisierte Verfahren bzw. – wenn erforderlich – für einzelne Anwendungen ist eine gesonderte Meldung mittels des folgenden Formulars zu erstellen. Zur Dokumentation und besseren Verwaltung ist die Nummerierung der Meldungen zweckmäßig. Unter Angabe der Nummern können später auch alle Änderungen bereits gemeldeter Verfahren oder Anwendungen durchgeführt werden.

<table>
<tr><td colspan="6">Meldeformular zur
automatisierten Verarbeitung nach § 4e BDSG
(bitte an den Datenschutzbeauftragten übersenden)</td></tr>
<tr><td colspan="6">Nur auszufüllen, wenn personenbezogenen Daten Hinweis Nr. 1verarbeitet werden!
Anmerkung: Soweit der Platz dieses Formulars nicht ausreicht fügen Sie bitte zusätzliche Anlagen bei.</td></tr>
<tr><td colspan="2">Projekt-Nr.: Hinweis Nr. 2</td><td>☐</td><td>Änderung bestehendes Verfahren</td><td>☐</td><td>Eigenentwickelte Software</td></tr>
<tr><td colspan="2">ggf. Einführungstermin: Hinweis Nr. 3</td><td>☐</td><td>neues Verfahren</td><td>☐</td><td>Standard- bzw. Kauf-Software</td></tr>
<tr><td colspan="6">1. Grundsätzliche Angaben zum Verfahren und zur Verantwortlichkeit.</td></tr>
<tr><td>1.1</td><td colspan="5">Bezeichnung und genaue Beschreibung des Verfahrens: Hinweis Nr. 4</td></tr>
<tr><td>1.2</td><td colspan="2">Fachbereich:</td><td colspan="2">Verantwortliche Führungskraft:</td><td>ggf. Stellen-Kennzeichen:</td></tr>
<tr><td>1.3</td><td colspan="4">Ausfüllende Person:</td><td>Telefon-Nummer:</td></tr>
<tr><td>1.4</td><td colspan="4">Name u. Anschrift des Auftragnehmers, wenn Auftragsdatenverarbeitung nach § 11 BDSG:</td><td>Vertrags-Nummer:</td></tr>
<tr><td colspan="6">2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung Hinweis Nr. 5</td></tr>
<tr><td>2.1</td><td colspan="5">Zweckbestimmung</td></tr>
<tr><td>2.2</td><td colspan="5">Rechtsgrundlage bitte ankreuzen soweit zutreffend und erläutern</td></tr>
<tr><td></td><td colspan="5">☐ Vertrag oder Vertragsanbahnung mit dem Betroffenen</td></tr>
<tr><td></td><td colspan="3">☐ Einwilligung des Betroffenen</td><td colspan="2">☐ Vorrangige Rechtsvorschriften</td></tr>
<tr><td></td><td colspan="3">☐ Interessenabwägung</td><td colspan="2">☐ Sonstiges (bitte erläutern)</td></tr>
<tr><td></td><td colspan="5">Erläuterungen:</td></tr>
</table>

3. a	**Art der gespeicherten Daten/ Datenkategorien** Hinweis Nr. 6	**Kreis der betroffenen Personengruppen** Hinweis Nr. 7

3. b	**Welche besonderen Arten von Daten werden verarbeitet?** Hinweis Nr. 8	
	☐ Daten zur Gesundheit	
	☐ Daten zum Sexualleben	
	☐ Daten über rassische und ethnische Herkunft	
	☐ Daten zu politischen Meinungen	
	☐ Daten zu religiösen oder philosophischen Überzeugungen	
	☐ Daten zur Gewerkschaftszugehörigkeit	
	☐ **Keine dieser Daten**	
	Rechtsgrundlage für diese besonderen Daten (bitte ankreuzen soweit zutreffend)	
	☐ Vertrag oder Vertragsanbahnung mit dem Betroffenen	
	☐ Einwilligung des Betroffenen	☐ Vorrangige Rechtsvorschriften
	☐ Interessenabwägung	☐ Sonstiges (bitte erläutern)
	Erläuterungen	

4. Art übermittelter Daten und deren Empfänger Hinweis Nr. 9

Interne Empfänger innerhalb der selben juristischen Person

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

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

Externe Stelle	Art der Daten	Zweck der Daten-Mitteilung

Geplante Datenübermittlung in Drittstaaten (außerhalb der EU)

Welcher Staat	Art der Daten	Zweck der Daten-Mitteilung

5. Regelfristen für die Löschung der Daten Hinweis Nr. 10

Ist eine fristabhängige Löschung vorgesehen?

☐ Ja ☐ Nein

6. Zugriffsberechtigte Personengruppen (Berechtigungsgruppen) Hinweis Nr. 11

Die Berechtigungen werden über das Berechtigungsverfahren in SAP administriert. ☐ Ja ☐ Nein
Die Berechtigungen werden über ein eigenes Berechtigungsverfahren in der Anwendung administriert. ☐ Ja ☐ Nein
7. Technische und organisatorische Maßnahmen (§ 9 BDSG)
Hinsichtlich der Datensicherheitsmaßnahmen wurde der Bereich IT-Sicherheit eingebunden ☐ Ja ☐ Nein
Die Maßnahmen entsprechen dem allgemeinen Unternehmens-IT-Sicherheitskonzept ☐ Ja ☐ Nein

Falls Nein, bitte Angaben zu den folgenden Maßnahmen ergänzen: Hinweis Nr. 12	**Termin**
Zutrittskontrolle	
Zugangskontrolle	
Zugriffskontrolle	
Weitergabekontrolle	
Eingangskontrolle	
Auftragskontrolle	
Verfügbarkeitskontrolle	
Trennungsgebot	

Datum: *Unterschrift der Führungskraft:*

Unterschrift der ausfüllenden Person:

5.3 Formular “Interner Prüfvermerk des Datenschutzbeauftragten“

(Nur von dem Bereich Datenschutz auszufüllen)

Projekt-Nr.		
	Datum	Namenszeichen
1. Vorgang geprüft		
1. Vorabkontrolle erforderlich ☐ ja ☐ nein		
2. Falls Vorabkontrolle erforderlich, Ergebnis:		
3. Wiedervorlage für Verfahrensregister zum Einführungszeitpunkt und Überprüfung der Einführung		
4. Zuordnung und Kontrolle der Auswirkungen auf die interne Verfahrensübersicht durchgeführt.; ggf. Anpassung.		
5. Kontrolle der Auswirkungen auf das öffentliche Verfahrensverzeichnis durchgeführt.; ggf. Anpassung.		
6. Ablage beim Datenschutz		

Anlage 6: Erläuterungen zu den Formularen 5.1 – 5.3

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, Kfz-Kennzeichen, Konto-Nr., Versicherungs- oder Personal-Nr., Beruf, Hausbesitzer.

Hinweis Nr. 2
Projektnummer
Angabe der Projektnummer bzw. der Systemnummer bei bereits implementierten Verfahren/Anwendungen; hier kann statt der Projektnummer auch ein anderer Ordnungsbegriff aufgenommen werden.

Hinweis Nr. 3
Einführungstermin
Geplanter Einführungstermin (Projekte) oder tatsächlicher Einführungstermin.

Hinweis Nr. 4
Beschreibung des Verfahrens
Genaue Kennzeichnung des Verfahrens mit Mitteln des allgemeinen Sprachgebrauchs und Hinweisen zur Verarbeitung personenbezogener Daten

Hinweis Nr. 5
Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung
Zieldefinition der Verarbeitung personenbezogener Daten und Nennung der darauf gerichteten rechtlichen Grundlage (Prinzip des Verarbeitungsverbots mit Erlaubnisvorbehalt)

Dies kann sein z.B. Datenverarbeitung zum Zweck der Übermittlung (Adresshandel, Erteilung von Wirtschaftsauskünften), Datenverarbeitung zum Zweck der anonymisierten Übermittlung (Markt- und Meinungsforschung).

Hinweis Nr. 6
Beispiele für **Datenkategorien**: Personaldaten, Kundendaten, Identifikations- und Adressdaten, Vertragsstammdaten, Kontokorrentdaten, IT-Nutzungsdaten.

Hinweis Nr. 7
Betroffene Personengruppen
Nennung der durch die Verarbeitung betroffener Personengruppen, z.B. Mitarbeitergruppen, Berater, Kunden, Lieferanten

betroffene Personengruppen kommen z.B. Kunden, Arbeitnehmer, Patienten, Schuldner, Versicherungsnehmer, Interessenten usw. in Betracht.

Hinweis Nr. 8
Diese „**besondere Arten** personenbezogener Daten“ ergeben sich aus § 3 Abs. 9 BDSG.

Hinweis Nr. 9
Datenübermittlung
Zweck und Empfänger personenbezogener Daten zur Weiterverarbeitung bzw. Nutzung

"**Empfänge**r" ist jede Person oder Stelle, die Daten erhält, z.B. Vertragspartner, Kunden, Behörden, Versicherungen, ärztliches Personal, Auftragsdatenverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter) usw.

§ 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. 10

Regelfristen für Datenlöschung

Darstellung der internen Löschvorschriften

Hier ist der Zeitraum anzugeben, nach dessen Ablauf die Daten gelöscht werden. Zu beachten ist in diesem Zusammenhang, dass nach § 35 Abs. 2 Nr. 4 BDSG eine Überprüfung spätestens vier Jahre nach der Einspeicherung erforderlich ist, sofern keine Spezialvorschriften einschlägig sind.

Hinweis Nr. 11

Zugriffsberechtigte Personengruppen

Skizzierung des Berechtigungsverfahrens und Nennung der berechtigten Gruppen.

Hinweis Nr. 12

Technische und organisatorische Maßnahmen (§ 9 BDSG)

Beschreibung der Schutzmaßnahmen im Hinblick auf die im BDSG genannten acht Schutzziele. Im Fall einer festgelegten betrieblichen Sicherheitspolitik im Unternehmen erfolgt alternativ der Hinweis auf die Abstimmung mit der Organisationseinheit „IT-Sicherheit“.

Die technischen und organisatorischen Maßnahmen zur angemessenen Sicherung der Daten vor Missbrauch und Verlust beinhalten entsprechend dem Bundesdatenschutzgesetz insbesondere

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (**Zutrittskontrolle**, z. B. beim Zutritt zu IT-Räumen wie Serverräumen etc.),

- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),

- dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),

- dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

- dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),

- dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle),**

- dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),

- dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (**Trennungskontrolle**).

Teil 6: English Summary: Data Privacy Application Registration

6 a) Preamble

This document is a summary of a guideline, which should help to provide an application register as a tool to achieve transparency of personal data processing within a company.
The object of the Application Register is to demonstrate

- which personal data
- using which automatic procedures
- processed or used in which manner
- protected by which data privacy measures

The Application Register is an essential element of the data privacy management system within companies.

According to the EU directive 95/46/EC, “on the protection of individuals with regard to the processing of personal data and on the free movement of such data”, section IX, there is an obligation to notify the supervisory authority before carrying out any wholly or partly automatic processing operation. A simplification is possible under the condition “keeping the register of processing operations …” This is the framework for the notification rules.
Even if the national law doesn´t require to provide such a register it is helpful as a basis for internal and external audits, as a tool for the responsible persons to manage data privacy issues and to be able to inform requesting individuals.

6 b) Who is responsible?

The data privacy laws address the executive management of the companies as the guarantors for data privacy issues. In fact the leader of the business departments are the owner of the data and against this background they must provide a project description for each new IT-system or for significant modifications of existing IT-systems within their area of accountability (a model template for such a notification is attached as annex 1). The application descriptions of the various departments should be coordinated and checked by the management or respective by the Data Privacy Officer. Based on this detailed information the responsible coordinator (e.g. Data Privacy Officer) provides the official Application Register for public needs (an example is attached as annex 2). This summarized information is sufficient to meet the demands of the concerned persons. The description of implemented data security measures is excluded in this case.

6 c) What is the minimum content of the application register?

To give a general review to the concerned individuals and the supervisory authority the following information is necessary:

- name and address of the responsible company
- names of the executive management members
- name of the head of IT and of the Data Privacy Officer (when implemented)
- the purpose of data processing and using
- the affected persons/groups
- data recipients
- planned data transfer to a third party country
- strategy for deletion of personal data

6 d) What are the steps to establish an application register?

The setup of an application register takes place within several phases:

The sensitization phase:
The employees in general are informed about the legal requirements regarding data privacy within business processes by mailings or by intranet or in context with other internal information.

The information phase:
The departments nominate employees, who are the experts for the business processes and applications within their area (business architect). These persons are trained in working out application descriptions in view of data privacy issues.

The inquiry phase:
Dependent on the size of the company the information collection will take place within a dialog between the application owner and the Data Privacy Officer or by a formal request following the paradigm in annex 1.

The clearing phase:
According to experience there are a lot of further inquiries while working out the descriptions. Dependent on the volume the implementation of a temporary hotline can be helpful.

The assessment phase:
The various application descriptions of the business groups have to be structured, verified and with regard to the official application register summarized by the Data Privacy Officer

The enhancement phase:
Extending the documentation as a result of changes in regard to processes, access rights, security measures, business scope etc. Arranging audits if applicable together with internal control.

Profil
Arbeitskreis Datenschutz

Datenschutz ist ein wichtiger Akzeptanzfaktor der Informationsgesellschaft. Seine rechtliche Gestaltung beeinflusst die Entwicklung einer modernen Wirtschaft. Er ist der entscheidende Vertrauensfaktor, der es ermöglicht, in der Informationsgesellschaft personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen. Insbesondere beim elektronischen Handel und der elektronischen Verwaltung kann Datenschutz das notwendige Vertrauen in die elektronische Kommunikation schaffen und verbreiteten Befürchtungen vor Missbrauch entgegenwirken. Ein moderner und technikadäquater Datenschutz ist damit auch ein bedeutender Wettbewerbsvorteil und Standortfaktor.

Dem trägt das bisherige Datenschutzrecht in Deutschland nur bedingt Rechnung. Es ist auch nach seiner Novellierung immer noch zu sehr auf das Konzept der räumlich abgegrenzten Datenverarbeitung fixiert, nimmt neue Formen personenbezogener Daten und deren Verarbeitung nur ungenügend auf und berücksichtigt nicht ausreichend die Chancen neuer Techniken der Datenverarbeitung. Darüber hinaus ist es in seinen Formulierungen häufig widersprüchlich und durch seine Normierung in Hunderten von speziellen Gesetzen unübersichtlich und schwer zu handhaben.

Für die BITKOM-Mitglieder ist nicht nur die datenschutzrechtliche Einbettung ihrer Geschäftsmodelle von täglicher Relevanz, sondern auch die Fragen des unternehmensinternen Datenschutzes. Der Umgang mit Mitarbeiterdaten, die Nutzung moderner Kommunikationsmittel am Arbeitsplatz und der konzerninterne Datenaustausch stellen die Unternehmen vor vielfältige Herausforderungen.

Aufgaben und Ziele

- BITKOM fordert ein datenschutzrechtliches Regelwerk, das am Wert und den Erfordernissen eines modernen Datenschutzes ausgerichtet ist.
- Der Arbeitskreis dient zum einen dem Informations- und Wissensaustausch der BITKOM-Mitglieder, zum anderen unterhält und fördert der Arbeitskreis den Kontakt zu den auf öffentlicher und staatlicher Seite verantwortlichen Entscheidungsträgern.

Aktivitäten

- Erarbeitung von Stellungnahmen zu aktuellen datenschutzrechtlichen Gesetzgebungsverfahren und Problemen.
- Aktive Beteiligung an den im Bereich Datenschutz erforderlichen Änderungen.
- Zusammenarbeit mit benachbarten BITKOM Gremien, insbesondere aus dem Bereich der Medienpolitik
- Entwicklung vertraglicher Lösungskonzepte für die Auftragsdatenverarbeitung.
- Erstellung von Publikationen und Praxishilfen
- Veranstaltung von Workshops
- Kritische Begleitung der Rechtsentwicklung im Bereich Datenschutz

Themen (Auswahl)

- RFID
- VoIP
- Datenschutzaudit (-Gesetz) und Gütesiegel
- Auftragsdatenverarbeitung
- Customer Relation Management
- Nutzung von Internet und Email am Arbeitsplatz
- Datentransfer in Drittländer
- Betrieblicher Datenschutz
- Schulungstools
- Arbeitnehmerdatenschutz
- BDSG in der Fassung von 05/2002
- Zweite Stufe der Novellierung des BDSG
- Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, 97/66/EG
- Neufassung der Richtlinie 97/66/EG
- Evaluation der Richtlinie 95/46/EG
- Umsetzung der Richtlinie 02/58/EG

Vorsitzende:
Ulrike Schroth, T-Systems Enterprise Services GmbH
Stellvertretender Vorsitzender:
Ralf Maruhn, Nokia GmbH

Ihr Ansprechpartner bei BITKOM:

Dr. Kai Kuhlmann
☎ 030/27576-131 fax 030/27576-139
k.kuhlmann@bitkom.org


BITKOM