Ausfüllhinweise für die Erstellung einer Verfahrensdokumentation

In § 4g Abs. 2 Satz 1 i.V.m. § 4e Satz 1 BDSG werden die in die Übersicht aufzunehmenden Angaben verbindlich und abschließend aufgezählt.

Teil 1 - zu veröffentlichende Angaben gem. § 4g Abs. 2 S. 1 i.V.m. § 4e S. 1 BDSG

1. Name oder Firma der verantwortlichen Stelle:

Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

2. Vertretung
Namen der Inhaber, Geschäftsführer oder sonstigen berufenen Leiter sowie Namen der mit der Leitung der Datenverarbeitung beauftragten Personen:

Die Personen sind namentlich zu benennen.

3. Anschrift der verantwortlichen Stelle:

Angabe der postalischen Adresse wie vorgegeben.

4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder –nutzung:

Diese Angaben sind für jedes einzelne Verfahren separat darzulegen. Das Verfahren ist dabei eindeutig zu bezeichnen. Über die Bezeichnung muss sich das Verfahren im Datenverarbeitungssystem der verantwortlichen Stelle oder eines beauftragten Auftragnehmers identifizieren lassen.

Der Zweck der Datenverarbeitung ist so präzise wie möglich zu benennen.
Nach § 4 Abs. 1 BDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene, d.h. die Person, deren Daten verarbeitet werden sollen, eingewilligt hat. Im Verfahrensverzeichnis ist daher zu dokumentieren, ob die Verarbeitung aufgrund einer Einwilligung oder aufgrund einer Rechtsvorschrift (mit Angabe des einschlägigen Paragraphen) erfolgt.

5. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien:

Hierzu zählen z.B.: Mitarbeiterdaten, Kundendaten, Lieferantendaten
Bei der Darstellung ist Bezug auf die Angaben zu Ziff. 4 zu nehmen, indem die personenbezogenen Daten bzw. Datenkategorien getrennt nach den einzelnen Zweckbestimmungen stichwortartig aufgeführt werden. Dabei sind Differenzierungen hinsichtlich der betroffenen Personengruppen vorzunehmen.
Betroffene Personengruppen sind die natürlichen Personen, deren Daten mit Hilfe des Verfahrens verarbeitet werden. Der Kreis der Betroffenen ist möglichst präzise zu bezeichnen.

Einzelmerkmale können dabei zu einem Sammelmerkmal zusammengefasst werden. Bei der Bildung von Sammelmerkmalen ist allerdings darauf zu achten, dass diese noch aussagekräftig bleiben. So dürfen einerseits die Begriffe nicht zu allgemein sein, weil sonst die Transparenz über den Umfang der Datenspeicherung verloren ginge. Andererseits sollten die gewählten Begriffe so flexibel sein, dass nicht jede kleine Änderung am Verfahren eine Änderung am Verfahrensverzeichnis nach sich zieht.

Unter dem Begriff „Daten“ werden „personenbezogene Daten“ i.S.d. § 3 Abs. 1 BDSG verstanden, also Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, z.B. Name, Geburtsdatum, Anschrift, Einkommen, Kfz-Kennzeichen, Konto-Nr. etc.

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können:

Empfänger ist jede Person oder Stelle, die Daten erhält, also nicht nur eine andere verantwortliche Stelle, sondern z. B. auch Auftragnehmer oder Filialen.
Hierzu zählen u. a. Vertragspartner, Behörden, Versicherungen, Auftragsdatenverarbeiter. Auch Stellen mit Online-Datenzugriff zählen als Empfänger.

7. Regelfristen für die Löschung der Daten:

Wer personenbezogene Daten mit Hilfe eines automatisierten Verfahrens verarbeitet, muss festlegen, wann welche Datenarten zu sperren oder zu löschen sind.
Im Bundesdatenschutzgesetz gibt es spezifische Regelungen wie die unverzügliche Löschung nach Zweckerreichung von Daten aus einer Videoüberwachung aus § 6b Abs. 5 BDSG, sowie die allgemeine Prüffrist aus § 35 Abs. 2 Nr. 4 BDSG, wonach spätestens vier Jahre nach der Einspeicherung eine Überprüfung erforderlich ist.
Fristen können sich darüber hinaus auch aus anderen Bestimmungen ergeben, wie z. B. aus der Abgabenordnung.

8. Datenübermittlung in Drittstaaten:

Hier sind die Übermittlungen, auch soweit bislang nur geplant, in Drittstaaten (Nicht-EU-Länder bzw. Nicht-EWR-Länder) anzugeben und zu begründen.
Dabei sind der Name der Drittstaaten und die übermittelten Daten zu benennen.

9. Allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind:

Hinweis: Diese Angabe muss und sollte in der Regel vom Unternehmen nicht öffentlich gemacht werden!

Nach § 9 BDSG muss die verantwortliche Stelle technische und organisatorische Sicherheitsmaßnahmen treffen, um eine datenschutzgerechte Verarbeitung personenbezogener Daten sicherzustellen.
Die Übersicht enthält eine allgemeine Beschreibung der eingesetzten Hardware, der Vernetzung und der Software. So wird die technische Infrastruktur dokumentiert. Die Beschreibung sollte erkennen lassen, welches Betriebssystem und welche Anwendungen auf wie vielen der eingesetzten Clients, Server, sowie etwa vorhandenen unvernetzten PC eingesetzt wird. Auch die Anbindung an die „Außenwelt“ mit den jeweils getroffenen Sicherungsmaßnahmen ist darzustellen.

Darüber hinaus sind entsprechend der Anlage zu § 9 S. 1 die Maßnahmen, welche zum Schutz der Daten oder Datenkategorien getroffen wurden, zu konkretisieren.
Dies sind im einzelnen:

Zutrittskontrolle
Unbefugten ist der Zutritt zu den Datenverarbeitungsanlagen, auf denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Diese Kontrolle bezieht sich auf den physischen Zutritt. Er kann z. B. durch verschlossene Türen zum Serverraum oder durch den Einsatz eines Pförtners bewerkstelligt werden.

Zugangskontrolle
Es ist zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden können.

Die Zugangskontrolle wird am Computer üblicherweise durch die Eingabe von Login-Namen und Passwort realisiert. Sie kann aber auch mit Magnet- oder Chipkarten sichergestellt werden.

Zugriffskontrolle
Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Außerdem muss gewährleistet sein, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Diese Befugnis zum Zugriff kann sich zum Beispiel bei Mitarbeitern aus der innerbetrieblichen Organisation ergeben. Umgesetzt werden kann sie im EDV-Bereich z. B. durch differenzierte Berechtigungen bei der Nutzung von Software. Ein Beispiel hierfür wäre, dass Daten der Buchhaltung nur von dieser selbst, aber nicht von der Vertriebsabteilung eingesehen werden. Die Zugriffskontrolle ist getrennt zu betrachten von Zutrittskontrolle und Zugangskontrolle.

Weitergabekontrolle
Hiermit soll verhindert werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Zudem soll überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen der Datenübertragung vorgesehen ist.

Die Weitergabekontrolle betrifft deswegen in der Praxis insbesondere Daten, die über Netzwerke fließen. E-Mails, die personenbezogene Daten enthalten, sind im Rahmen der Weitergabekontrolle zu schützen (in der Praxis oftmals mittels Verschlüsselung).

Eingabekontrolle
Unter Eingabekontrolle versteht man, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungsanlagen eingegeben, verändert oder entfernt worden sind.

Dies geschieht in der Regel durch eine automatische Protokollierung der Eingaben in Logfiles. Elemente einer Protokollierung sind der betroffene Datensatz, die Art der Aktivität (Anlage, Veränderung, Löschung des Datensatzes), der Zeitpunkt der Aktivität bzw. des Ereignisses sowie ausführende Person (Benutzerkennzeichen). Die Eingabekontrolle setzt eine funktionierende Zugangskontrolle voraus.

Auftragskontrolle

Die Kontrolle ist nur anwendbar, wenn eine Auftragsdatenverarbeitung nach § 11 BDSG vorliegt. Ein Auftrag liegt dann vor, wenn die Daten durch eine andere juristische Person nach genauen Vorgaben verarbeitet werden (Beispiel: externe Buchhaltung).

In diesem Fall ist vertraglich und ggfs. durch Kontrollen sicherzustellen, dass die personenbezogenen Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Verfügbarkeitskontrolle
Unter Verfügbarkeitskontrolle versteht man, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen sind.

In der Regel geschieht dies durch fachgerechte regelmäßige Datensicherungen, aber auch durch einen Notfallplan, Virenschutz und andere Maßnahmen.

Trennungsgebot
Das Trennungsgebot ist ein Grundsatz, nach dem zu unterschiedlichen Zwecken erhobene Daten auch nur getrennt verarbeitet werden dürfen.

Deshalb ist z. B. der Test-Datenbestand strikt zu trennen vom Produktiv-Datenbestand.

10. Angabe der zugriffsberechtigten Personen:

Hinweis: Diese Angabe muss und sollte in der Regel vom Unternehmen nicht öffentlich gemacht werden!

Zugriffsberechtigte Personen sind grundsätzlich die Beschäftigten der verantwortlichen Stelle, die auf Grund ihrer Position oder Funktion Zugang zu bestimmten dafür relevanten Daten haben. Die übrigen Personen werden bereits als Dritte unter Ziff. 6 erfasst.
Auf eine namentliche Nennung kann dabei, auch wegen des sich daraus ergebenen hohen Änderungsbedarfs des Verzeichnisses, zugunsten einer Funktionsbezeichnung, verzichtet werden. Sofern die zugriffsberechtigten Mitarbeiter auf unterschiedliche Datenarten zugreifen können, sollte auch dies erkennbar sein.