Ausfüllhinweise zur Dokumentation von Verarbeitungstätigkeiten

**Bitte beachten Sie beim Ausfüllen des Dokuments darauf, keine personenbezogenen Daten zu nennen!**

**Checkboxen können mit einem Doppelklick auf „aktiviert“ oder „deaktiviert“ gesetzt werden.**

**Verfahrensname:** Wählen Sie bitte eine aussagekräftige Bezeichnung der Verarbeitungstätigkeit inklusive Nennung der verantwortlichen Abteilung. Als Verarbeitungstätigkeit wird im Allgemeinen ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden. Es ist zu empfehlen, den Namen der jeweiligen Verarbeitungstätigkeit von dem Verarbeitungszweck ausgehend festzulegen (bspw. „Personalaktenführung“/“Stammdaten“, „Lohn-, Gehalts- und Bezügeabrechnung“ usw.).

**Zu Kapitel 1.:** Bitte beschreiben Sie in wenigen Sätzen das zu dokumentierende Verfahren. Diese Kurzbeschreibung dient als grundlegende Vorstellung und steckt den Rahmen dieser Dokumentation ab.

**Zu Kapitel 2.:** Dieses Kapitel dokumentiert, welche Daten auf welche Weise verarbeitet werden.

Zu 2.1.1. Welche Personen, Gruppen oder Rollen sind an dem Verfahren beteiligt? Die im Dokument genannten Betroffenengruppen dienen lediglich als Beispiele zur Orientierung, nicht Zutreffendes bitte löschen.

Zu 2.1.2. Nähere Unterscheidung zwischen personenbezogenen Daten und weiteren Informationen ohne Personenbezug, die in dem Verfahren verarbeitet werden. Alle im Verfahren verarbeiteten Daten sind in der Regel schutzbedürftig, erfordern aber unterschiedliche Dokumentationspflichten.

Definition von personenbezogenen Daten: *Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person. Hierzu zählen auch personenbeziehbare Daten, also Daten, bei denen ein Personenbezug hergestellt werden kann (bspw. IP-Adressen).*

Hinweis: Bitte geben Sie hier lediglich Kategorien von personenbezogenen Daten an, keine konkreten individuellen Daten.

Falls keine personenbezogenen Daten verarbeitet werden, können die folgenden Abschnitte gelöscht und mit Abschnitt 3 fortgefahren werden.

Falls personenbezogene Daten verarbeitet werden, nennen Sie bitte die Arten / Kategorien von personenbezogenen Daten. Die im Dokument genannten Kategorien dienen lediglich als Beispiele zur Orientierung, nicht Zutreffendes bitte löschen.

Zu 2.2. Auflistung der Verarbeitungszwecke: Nennen Sie hier die Gründe / den Zweck für die Verarbeitung von personenbezogenen Daten und die zugrundeliegenden Rechtsgrundlagen. Stellen Sie sich hier die Frage, warum bestimmte Daten erhoben werden und ob diese Daten für den konkreten Vorgang wirklich erforderlich sind. Jede / jeder Betroffene hat Auskunftsansprüche zu ihren / seinen verarbeiteten personenbezogenen Daten und auf welchen Rechtsgrundlagen diese Verarbeitung stattfindet. Die Dokumentation der Rechtsgrundlagen erleichtert somit die Erteilung von entsprechenden Auskünften. Die genannten Verarbeitungszwecke sind ohne eine entsprechende Rechtsgrundlage nicht zulässig (Verbot mit Erlaubnisvorbehalt).

Beispiele für typische Rechtsgrundlagen im Hochschul- und Verwaltungsumfeld:

- Einwilligung

- Zur Erfüllung eines öffentlichen Auftrags

- Forschungszwecke

- gesetzliche Rechtsgrundlagen z.B.

* Gesetz über die Statistik für Bundeszwecke vom 22.1.1987 (BGBl. I, S. 462, 565) i.V.m. § 111 Abs. 7 HmbHG
* Gesetz über die Statistik für das Hochschulwesen sowie für die Berufsakademie vom 2.11.1990 (BGBl. I, S. 2414), insbesondere § 3
* Hamburgisches Datenschutzgesetz vom 18. Mai 2018, insbesondere § 11
* Hamburgisches Statistikgesetz vom 19.3.1991 (HmbGVBl. 1991, S. 79)
* Hamburgisches Hochschulgesetz vom 18.7.2001 (HmbGVBl. 2001, S. 171), insbesondere § 111 Abs. 1 und 7
* Gesetz über die Zulassung zum Hochschulstudium in Hamburg vom 28.12.2004 (HmbGVBl. 2004, S. 515)
* Hamburgisches Archivgesetz vom 21.1.1991 (HmbGVBl. 4991, S. 7), insbesondere § 3
* Satzung zum Studium (Immatrikulations- und Zulassungsordnungen)
* Prüfungsordnungen
* Satzung über die Erhebung und Verarbeitung personenbezogener Daten gemäß § 111 Abs. 1, 3 und 7 HmbHG vom 25.8.2004 in Verbindung mit der Anlage 1, insbesondere § 1
* Aktenordnung
* Verordnung (EU) Nr. 912/2013 der Kommission vom 23.9.2013 zur Durchführung der Verordnung (EG) Nr. 452/2008 des Europäischen Parlaments und des Rates über die Erstellung und die Entwicklung von Statistiken über Bildung und lebenslanges Lernen im Hinblick auf Statistiken über die Systeme der allgemeinen und beruflichen Bildung (ABl. L 252 vom 24.9.2013, S. 5) und der Durchführungsverordnung (EU) Nr. 995/2012 der Kommission vom 26.10.2012 mit Durchführungsvorschriften zur Entscheidung Nr. 1608/2003/EG des Europäischen Parlaments und des Rates zur Erstellung und Entwicklung von Gemeinschaftsstatistiken über Wissenschaft und Technologie (ABl. L 299 vom 27.10.2012, S. 18) wird eine Bundesstatistik, teilweise als Studienverlaufsstatistik, durchgeführt

Die Rechtsgrundlagen sind in der jeweils gültigen Fassung zu verwenden.

Zu 2.3.: Art. 9 Abs. 1 DSGVO sagt aus: *„Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.“*

Ausnahmen hierfür sind unter bestimmten Umständen / Zweckbestimmungen möglich. Diese Ausnahmen sind in Art. 9 Abs. 2 DSGVO definiert (siehe <https://dsgvo-gesetz.de/> )

Zu 2.4.: Zunächst muss der Verantwortliche prüfen, ob im konkreten Fall die Durchführung einer Datenschutzfolgeabschätzung (DSFA) notwendig ist. Dies ist gemäß Art. 35 Abs. 1 DSGVO „insbesondere“ der Fall, wenn „aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten“ der Betroffenen besteht.

Der Verantwortliche muss also die Intensität der Beeinträchtigungen für Betroffene und die Risiken für die Ausübung von Grundrechten abschätzen. Wird festgestellt, dass durch den geplanten Verarbeitungsvorgang voraussichtlich die Beeinträchtigung nicht hoch und zudem kein hohes Risiko besteht, ist eine DSFA nicht zwingend durchzuführen. Entscheidet der Verantwortliche keine DSFA durchzuführen, ist diese Entscheidung unter Angabe der maßgeblichen Erwägungen zu dokumentieren. Von der Artikel-29-Arbeitsgruppe wurde jetzt ein Arbeitspapier mit Leitlinien veröffentlicht, wann eine solche Folgenabschätzung notwendig ist. Dieses Arbeitspapier ist von großer Bedeutung, da die [Artikel-29-Gruppe](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083) sich aus Vertretern der Aufsichtsbehörden der Mitgliedsstaaten zusammensetzt. Diese Behörden sollen durch die Erstellung von Positiv-und Negativlisten klarstellen, wann eine DSFA durchzuführen ist. Die Leitlinien sehen vor, dass die Verantwortlichen in bestimmten Fällen die unbedingte Pflicht haben, eine Folgenabschätzung durchzuführen. Die folgenden neun Kriterien deuten darauf hin, dass bei einer Datenverarbeitung voraussichtlich ein hohes Risiko besteht:

1. Bewertung und Einstufung (Scoring) einschließlich Prognosen und Profilerstellung

Laut Erwägungsgründen 71, 91 DSGVO liegt dies insbesondere vor, wenn die Arbeitsleistung, wirtschaftliche Situation, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel beurteilt werden. Die Artikel-29-Datenschutzgruppe benennt hier das typische Beispiel der Bank, die die Kreditwürdigkeit eines Kunden bewertet, aber auch Gentests zur Bestimmung von Krankheiten oder das Tracking von Webseiten-Besuchern.

2. Automatisch erfolgende Entscheidungen mit rechtlichen oder ähnlich signifikanten Auswirkungen für Betroffene

Bei automatischen Verarbeitungen droht eine Diskriminierung oder der Ausschluss bestimmter Individuen von Leistungen oder Angeboten, sodass diese besonders risikoreich sind.

3. Systematische Überwachung

Systematische Überwachung kann dazu führen, dass Daten von Betroffenen gesammelt werden, ohne dass ihnen dies oder die spätere Nutzung bewusst sind. Zudem ist es Individuen bei öffentlich zugänglichen Bereichen unter Umständen nicht möglich, diese zu umgehen.

4. Sensible personenbezogene Daten

Als sensibel sind insbesondere die die besonderen Kategorien von Daten gemäß Art. 9 Abs. 1 sowie Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO anzusehen. Nach der Artikel-29-Datenschutzgruppe fallen auch allgemeinere Daten, wie etwa Daten elektronischer Kommunikation, Aufenthaltsorte oder Finanzdaten unter dieses Kriterium. Dabei kann auch zu berücksichtigen sein, ob die Daten bereits öffentlich zugänglich sind.

5. Umfang der Verarbeitung

Zur Bestimmung, ob es sich um eine umfangreiche Datenverarbeitung handelt, empfiehlt die Artikel-29-Datenschutzgruppe in Anlehnung an Erwägungsgrund 91 zu berücksichtigen, wie viele Betroffene erfasst werden (entweder absolut oder als Anteil der betroffenen Mitglieder und Angehörigen der Hochschule), das Volumen der Daten und/oder die Breite der verschiedenen Daten, die verarbeitet werden, die Dauer oder der Bestand der Verarbeitungstätigkeit sowie die geografische Ausbreitung der Verarbeitungstätigkeit.

6. Vergleich oder Kombination von Datensätzen

Der Vergleich oder die Kombination von Datensätzen aus verschiedenen Quellen unter Einhaltung des Prinzips der Zweckbindung, die zu verschiedenen Zwecken von verschiedenen Verantwortlichen erhoben wurden, begegnet der Gefahr, dass er die vernünftigen Erwartungen der Betroffenen übersteigt.

7. Daten schutzbedürftiger natürlicher Personen

Aufgrund des gesteigerten Machtungleichgewichts zwischen den Betroffenen und dem Verantwortlichen, kann die Verarbeitung von besonders schutzbedürftigen Personen die Durchführung einer DSFA nötig machen. Dies ergibt sich daraus, dass sich die Person einer Verarbeitung ihrer Daten nicht erwehren kann und gilt u.a. für Arbeitnehmer, Kinder, Menschen mit geistigen Behinderungen, Asylsuchende, ältere Menschen, Patienten.

8. Einsatz innovativer Technologien oder neuartiger organisatorischer Lösungen

Der Einsatz neuartiger Technologien kann neue Formen der Datensammlung und -verarbeitung beinhalten, da ihre persönlichen oder sozialen Folgen noch nicht bekannt sind. Dies gilt etwa für die Kombination von Fingerabdrücken und Gesichtserkennung für bessere physische Zugangskontrollen oder bestimmte Anwendungen des Internets der Dinge, die einen erheblichen Einfluss auf den Alltag und die Privatsphäre der Betroffenen haben können.

9. Verhinderung, dass die betroffene Person ein Recht ausüben, eine Dienstleistung in Anspruch nehmen oder einen Vertrag abschließen kann

Dieses letzte Kriterium umfasst etwa die Verarbeitung in öffentlichen Bereichen, die Betroffene nicht vermeiden können oder die das Recht der Betroffenen ändern, einen Vertrag einzugehen oder Zugang zu einer Dienstleistung zu erlangen, etwa durch eine Bonitätsauskunft.

Die Artikel-29-Datenschutzgruppe geht davon aus, dass ein hohes Risiko wahrscheinlicher ist, je mehr dieser Kriterien ein Verarbeitungsvorgang erfüllt, weist aber ausdrücklich darauf hin, dass dies auch der Fall sein kann, wenn nur eines der Kriterien erfüllt ist. Die Analyse im Rahmen einer DSFA ist ausführlicher, als es die Risikodokumentation in Kapitel 3 vorsieht. Kapitel 3 enthält aber bereits ein paar wichtige Ansatzpunkte zur Risikominimierung. Weitere Informationen zur DSFA finden Sie hier:

<https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf>

Zu 2.5.: Hier soll dokumentiert werden, welche Gruppen / Kategorien/ Rollen / Dritte die personenbezogenen Daten einsehen können.

Zu 2.6.: Das Datenschutzrecht sieht den Grundsatz der Datensparsamkeit vor, d.h. dass nur die personenbezogenen Daten in dem Umfang verarbeitet werden, wie dies für den jeweiligen Zweck erforderlich ist und nicht darüber hinaus. Bitte nennen Sie hier eine Begründung warum der Umfang der aktuell verarbeiteten Daten reduziert werden kann oder warum nicht.

Zu. 2.7.: Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym (zumeist eine mehrstellige Buchstaben- oder Zahlenkombination, auch Code genannt) ersetzt, um die Feststellung der Identität des Betroffenen auszuschließen oder wesentlich zu erschweren. Bitte nennen Sie hier eine Begründung warum die personenbezogenen Daten pseudonymisiert werden können oder falls nicht, warum nicht.

Zu 2.8.: Die verfahrensverantwortlichen sollten Sperr- und Löschfristen für die in den Verfahren verarbeiteten personenbezogenen Daten kennen und entsprechend anwenden, soweit dies praktisch umsetzbar ist.

Zu 2.9.: Falls personenbezogene Daten weitergegeben werden, sollen die Empfängerkategorien hier dokumentiert werden. Da die personenbezogenen Daten auf der Empfängerseite ggf. nicht mehr auf dem gleichen Niveau geschützt sind, sieht die DSGVO vor, dass dies hier dokumentiert und überprüft wird. Jede Übermittlung personenbezogener Daten ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in Artikel 5 der DSGVO niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen der EU DSGVO eingehalten werden.

Eine Datenübermittlung in ein Drittland ist laut DSGVO nur dann zulässig, wenn geeignete Garantien für den Schutz der personenbezogenen Daten vorliegen (siehe Artikel 46 DSGVO). Die genannten Garantien sind nur Beispiele, bitte ggf. ergänzen und nicht Zutreffendes löschen.

Zu 2.10.: Hier soll dokumentiert werden, woher die zu verarbeitenden Daten stammen und ob eine Übernahme von Altdaten erforderlich ist. Ggf. muss dann geprüft werden, ob dieser Datenimport rechtlich zulässig ist oder nicht.

Zu 2.11.: Nennen Sie hier bitte die Rollen / Kategorien von Nutzern, die mit den Daten im Rahmen dieses Verfahrens arbeiten. Bitte keine Namen nennen.

**Zu Kapitel 3:** Daten müssen vor Schäden, Angriffen und ungewollten Veränderungen aller Art sinnvoll geschützt werden. Dies erfordert laut DSGVO bzw. generell aus Sicht der Informationssicherheit die Umsetzung von geeigneten technisch-organisatorischen Schutzmaßnahmen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Standards zur Herstellung eines IT-Grundschutzniveaus entwickelt und spricht dort vom „Schutzbedarf“ von Daten, Systemen und Räumen. Die hier betrachteten Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität können sich jeweils in ihren Schutzbedarfsanforderungen unterscheiden. Wie in dem Formular bereits beschrieben, gibt es drei Schutzbedarfskategorien (normal, hoch und sehr hoch) pro Schutzziel. Je höher der Schutzbedarf desto umfangreicher und wirkungsvoller müssen die dafür gewählten Schutzmaßnahmen sein. Eine gute Orientierung für den Schutzbedarf bietet eine Worst-Case-Betrachtung:

Vertraulichkeit: Welche Konsequenzen / Schadensauswirkungen hätte eine unberechtigte Veröffentlichung / Weitergabe an oder Einsichtnahme der Daten durch nicht berechtigte Personen?

Integrität: Welche Konsequenzen / Schadensauswirkungen hätten fehlerhafte Daten für die verarbeitende Organisation? Diese Fehler könnten durch menschliches Versagen oder durch fehlerhafte Soft- oder Hardware entstehen.

Verfügbarkeit: Welche Konsequenzen / Schadensauswirkungen hätte es, wenn berechtigte Benutzer nicht auf die Daten zugreifen könnten (z.B. durch Systemausfälle oder Denial-of-Service Angriffe)?

Bedenken Sie bitte, dass Schutzbedarf „normal“ keinesfalls bedeutet, dass keine Schutzmaßnahmen notwendig sind. Das BSI hat daher bewusst auf die Verwendung der Kategorie „gering“ oder „keine“ verzichtet. Folgende Beispielkategorien führt das BSI auf, die für eine Einordnung verwendet oder angepasst werden können:

|  |  |
| --- | --- |
| **Schutzbedarfskategorie „normal“** | |
| Verstoß gegen Gesetze/Vorschriften/Verträge | Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen.  Geringfügige Vertragsverletzungen mit geringen Konventionalstrafen (< X Euro). |
| Beeinträchtigung des informationellen Selbstbestimmungsrechts | Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen nicht beeinträchtigt werden kann. |
| Beeinträchtigung der persönlichen Unversehrtheit | Eine Beeinträchtigung erscheint nicht möglich. |
| Beeinträchtigung der Aufgabenerfüllung | Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden.  Die maximal tolerierbare Ausfallzeit von IT-Systemen kann bis zu 5 Arbeitstage betragen. |
| Negative Innen- oder Außenwirkung | Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. |
| Finanzielle Auswirkungen | Der finanzielle Schaden ist geringer als X Euro. |

|  |  |
| --- | --- |
| **Schutzbedarfskategorie „hoch“** | |
| Verstoß gegen Gesetze/Vorschriften/Verträge | Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen.  Vertragsverletzungen mit hohen Konventionalstrafen ( > X Euro). |
| Beeinträchtigung des informationellen Selbstbestimmungsrechts | Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann. |
| Beeinträchtigung der persönlichen Unversehrtheit | Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden. |
| Beeinträchtigung der Aufgabenerfüllung | Die Beeinträchtigung würde von einzelnen Betroffenen  Der Ausfall von IT-Systemen ist nur bis zu 2 Arbeitstagen tragbar. |
| Negative Innen- oder Außenwirkung | Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist erwarten. |
| Finanzielle Auswirkungen | Der finanzielle Schaden liegt zwischen X und Y Euro. |

|  |  |
| --- | --- |
| **Schutzbedarfskategorie „sehr hoch*“*** | |
| Verstoß gegen Gesetze/Vorschriften/Verträge | Fundamentaler Verstoß gegen Vorschriften und Gesetze.  Vertragsverletzungen, deren Haftungsschäden ruinös sind. |
| Beeinträchtigung des informationellen Selbstbestimmungsrechts | Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann. |
| Beeinträchtigung der persönlichen Unversehrtheit | Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich.  Gefahr für Leib und Leben. |
| Beeinträchtigung der Aufgabenerfüllung | Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden.  Ein IT-Systemausfall ist nur wenige Stunden tragbar. |
| Negative Innen- oder Außenwirkung | Eine landes- bzw. bundesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist denkbar. |
| Finanzielle Auswirkungen | Der finanzielle Schaden ist größer als X Euro. |

**Zu Kapitel 4. Verwendete IT-Infrastruktur**

4.1. Beteiligte Systeme und Anwendungen

Bspw:

- Office-Programme  
- spezielle Anwendungen  
- besondere Hardware

4.2 Tolerierbare Ausfallzeit

Geben Sie hier an, wie lange ein Ausfall der IT-Infrastruktur tolerierbar wäre (bspw. 1 Stunde, 4 Stunden, 1 Tag, 3 Tage, 1 Woche, …), bevor große Auswirkungen / Schäden entstehen würden.

4.3 Beschreibung der Vorgehensweise bei Änderung von Programmfunktionalitäten (Changemanagement)

Bspw.:

- Vorgehen bei Programmanpassungen

- Änderung von Programmparametern

- Deaktivierung von Masken oder Feldern

- Releasewechsel und Updates

- Abhängigkeiten von anderen IT-Anwendungen, …)

4.4 Nennen der Systembetreuer (Kategorie / Rolle)

Bspw.:

- Administratoren

- Externer Support

- Studentische Hilfskraft

4.5 Wer führt wie die Abnahme und Freigabe der IT-Anwendung(en) durch?

Bspw.:

- IT-Leitung

- Verfahrensverantwortliche

- Personalrat

- Datenschutzbeauftragter

- Informationssicherheitsbeauftragter

4.6 Wie und durch wen erfolgt die Schulung, Einweisung oder Unterrichtung und die Betreuung der betroffenen Anwender?

Bspw.:

- Administratoren

- Externe

-IT-Abteilung

Zu Kapitel 5:

Müssen im Zusammenhang mit dieser Verarbeitungstätigkeit weitere datenschutzrechtliche Verpflichtungen erfüllt werden? Dies ist zum Beispiel der Fall, wenn Webseiten verwendet werden (ggf. Datenschutzerklärung anpassen), falls Dritten personenbezogene Daten zur Verarbeitung überlassen werden oder wenn personenbezogene Daten erhoben werden (Informationspflichten einhalten). Ggf. müssen Einwilligungen eingeholt und verwaltet werden. Der Datenschutzbeauftragte kann bei allen Fragen zu diesen Themenbereichen unterstützen.

**Zu Kapitel 6:** Wann bzw. in welchen Fällen findet die nächste Überprüfung der Verfahrensdokumentation statt?

Mehrere Antworten möglich. Empfohlen wird eine Überprüfung mindestens alle 2 Jahre.